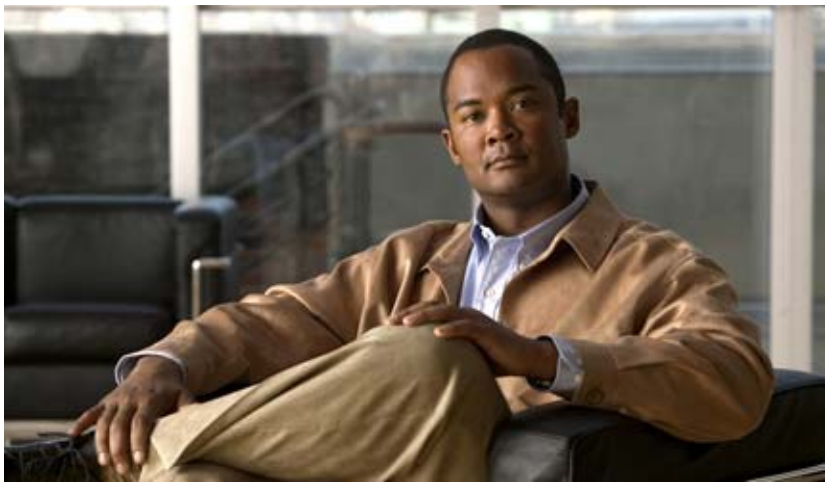


# Cisco Unified Messaging Gateway 1.0 CLI Administrator Guide

First released: November 2007
Last updated: April 13, 2010

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Customer Order Number: OL-13125-01

*Cisco Unified Messaging Gateway 1.0 CLI Administrator Guide*

# Notices

The following notices pertain to this software license.

# OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

## License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

#### OpenSSL License:



Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

**Original SSLeay License:**



This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

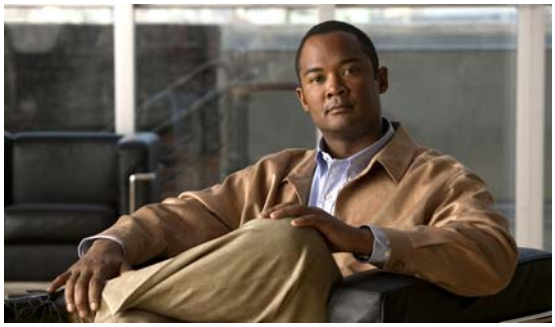
1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

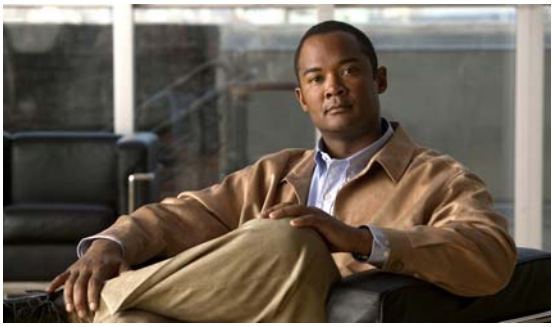
   The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".



The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].



# CONTENTS



# Cisco Unified Messaging Gateway 1.0 Feature Roadmap

**Last updated: April 13, 2010**

Cisco Unified Messaging Gateway (Cisco UMG) 1.0 provides a standards-based method of intelligently routing messages, exchanging subscriber and directory information, and providing interoperability within a messaging network. It acts as the central hub for Cisco Unity, Cisco Unity Express, and Avaya Interchange systems interfacing with legacy voice mail systems.

### Finding Support Information for Cisco Unified Messaging Gateway 1.0

This guide complements the *Cisco Unified Messaging Gateway 1.0 Command Reference*, the *Cisco Unified Messaging Gateway 1.0 Installation Guide* and the *Cisco Unified Messaging Gateway 1.0 Release Notes*. These publications can be found at http://www.cisco.com/en/US/products/

This guide does not provide information on the installation or configuration of Cisco routers, Cisco Unity Express, or Cisco Unity. Information on these products can be found at

Cisco routers at http://www.cisco.com/en/US/products/hw/routers/index.html

Cisco Unity Express at http://www.cisco.com/en/US/products/sw/voicesw/ps5520/index.html

Cisco Unity at http://www.cisco.com/en/US/products/sw/voicesw/ps5520/index.html.

# Feature List

Table 1 lists the Cisco UMG 1.0 features and maps them to the corresponding sections in this guide.

*Table 1 Cisco Unified Messaging Gateway 1.0 Features*

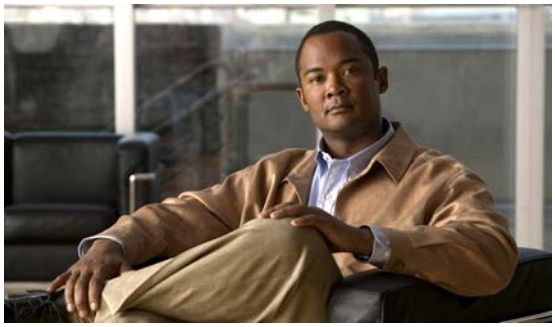
| Feature | Description of Benefit | Where Documented |
|---|---|---|
| **Able to integrate Cisco Unity Express, Cisco Unity, and 3rd party voice messaging system (Avaya Interchange)** | Cisco UMG supports:<br>• Cisco Unity Express only deployment<br>• Mixed Cisco Unity Express/Cisco Unity deployment<br>• Mixed Cisco Unity Express/Unity/3rd party Avaya Interchange deployment | "Configuring Endpoint Autoregistration Support" on page 28, and "Provisioning Endpoints Manually" on page 31 |
| **Accessible CLI** | Cisco UMG provides familiar management features such as configuration, provisioning, and support through a CLI that is similar to the Cisco IOS CLI, thereby reducing the learning curve and accelerating learning speed for network administrators and channel partners familiar with Cisco IOS software. | "Entering and Exiting the Command Environment" on page 15 |
| **Embedded Operating System** | Cisco UMG employs an industry-standard OS ideally suited for embedded applications. It enables a disk subsystem not provided by native Cisco IOS software.<br>This approach translates into efficient operation while providing a robust and protected operating environment behind Cisco IOS software. | Throughout |
| **Open messaging standards including VPIM and SMTP** | Cisco UMG supports VPIM networks with<br>• Cisco Unity Express 3.1 and later versions,<br>• Cisco Unity 4.05,<br>• Avaya Interchange 5.4. | Throughout |
| **Autoregistration for Cisco Unity Express 3.1 and later versions** | Cisco UMG enables simple, secure autoregistration with Cisco Unity Express 3.1 and later versions.<br>Secure autoregistration is accomplished through user name and password defined on Cisco UMG.<br>Cisco UMG supports restricting autoregistration to specific systems based on administrative needs.<br>Cisco UMG supplies reports on:<br>• Autoregistration attempts<br>• Failures<br>• Successes<br>Cisco UMG displays by CLI **show** commands:<br>• Registered endpoints<br>• Endpoints provisioned for registration and not currently registered. | "Configuring Endpoint Autoregistration Support" on page 28<br>"Provisioning Endpoints Manually" on page 31<br>"Blocking Endpoint Registration" on page 76<br>"Viewing Network Status" on page 53 |
| **Manual registration for Cisco Unity and 3rd party messaging systems** | Cisco UMG supports manual registration / provisioning for:<br>• Cisco Unity 4.05<br>• Third party voice mail systems (Avaya Interchange 5.4)<br>• Cisco Unity Express 3.1 and later versions. | "Provisioning Endpoints Manually" on page 31 |

*Table 1 Cisco Unified Messaging Gateway 1.0 Features (continued)*

| Feature | Description of Benefit | Where Documented |
|---|---|---|
| **Centralized VPIM routing** | Cisco UMG simplifies message routing and management by implementing a star topology for each messaging gateway and its associated endpoints, thereby obviating the need for fully-meshed networks between those endpoints. Each messaging gateway acts as a central hub for VPIM routing. | "Configuring Endpoint Autoregistration Support" on page 28<br>"Provisioning Endpoints Manually" on page 31 |
| **Automatic directory exchange and update** | Cisco UMG implements automatic directory exchange, instead of a static directory table. Messaging gateways are capable of automatically retrieving directory information from Cisco Unity Express 3.1 and later versions, as well as exchanging/updating directory information with the peer messaging gateways in the system. | "Forcing Data Convergence" on page 66 |
| **Multiple messaging operations support** | Cisco UMG supports Cisco Unity Express 3.1 and later versions message sending, forwarding, replying, vCard exchange, dial-by extension, and dial-by-name with spoken name enabled. | Throughout<br>"Revisiting the Installation Configuration" on page 20 |
| **Multiple address schemes support** | Cisco UMG supports the following address schemes:<br>• Site ID ('prefix') + extension<br>• E.164 address (10 digit dialing)<br>• Any numeric string length if it is unique in the messaging network. | Throughout |
| **System Distribution List (SDL) and System Broadcast Message (SBM) management** | Cisco UMG can manage (create/delete/permit/reject/publish) System Distribution Lists (SDLs) and System Broadcast Messages (SBMs) across multiple voice mail systems within the Cisco Unified Messaging network. | "Managing System Broadcasts" on page 71<br>"Managing System Distribution Lists" on page 67 |
| **Header manipulation and message translation** | Cisco UMG supports SMTP and message header manipulation to enable messages to be delivered across different messaging systems (between Cisco Unity/Cisco Unity Express/Avaya Interchange). | "Message Transmission" on page 83 |
| **Redundancy** | Cisco UMG provides a self-healing network topology through the primary-secondary active/active failover model.<br>**Note** Avaya Interchange can only communicate with a single remote messaging gateway, and therefore no failover support can be provided for it. | "Configuring Peer Messaging Gateways" on page 24, "Configuring Endpoint Autoregistration Support" on page 28, and "Provisioning Endpoints Manually" on page 31 |
| **NDR and DDR** | Cisco UMG is capable of generating and delivering non-delivery receipts (NDRs) and delayed delivery receipts DDRs with configurable timeouts. | "Message Handling" on page 26 |
| **NAT Support** | Cisco UMG supports message delivery through NAT. You can configure the NAT table on the messaging gateway to map internal and external IP addresses. | "Setting Up NAT Entries" on page 36 |
| **Scalability** | A fully-meshed Cisco UMG system can support up to 20 messaging gateways (including both primary and secondary messaging gateways) with a total of up to 500,000 subscribers. | "Functional Outline" on page 6 |

*Table 1 Cisco Unified Messaging Gateway 1.0 Features (continued)*

| Feature | Description of Benefit | Where Documented |
|---|---|---|
| **Backup and Restore** | Cisco UMG has backup and restore capabilities. Backup and restore will include the data from both local configuration and from directory exchange/update across the messaging network. | "Backing Up and Restoring Data" on page 45 |
| **System provisioning and management capability** | Cisco UMG supplies logging and tracing capabilities. With these CLI commands the administrator can<br>• troubleshoot<br>• monitor a specific system module on certain activities<br>• log the tracing message to a remote FTP server, or<br>• log the events to a remote syslog server<br>Cisco UMG can load and save configurations the same way as Cisco IOS routers and switches can.<br>Cisco UMG supports software upgrades from/to major releases.<br>Cisco UMG provides startup and shutdown capabilities exactly like Cisco Unity Express and Cisco IOS software. | "Monitoring the Cisco Unified Messaging Gateway System" on page 53, and "Troubleshooting" on page 79 |
| **Cisco Unity Express TUI and VVE New Prompts** | Cisco UMG provides additional prompts on the Cisco Unity Express telephone user interface (TUI) and VoiceView Express (VVE) applications with the option of Global Directory Lookup when the local Cisco Unity Express endpoint does not have the requisite information saved in its cache. | See Cisco Unity Express documentation. |
| **Spoken-name confirmation** | Cisco UMG provides spoken-name confirmation for all local and remote recipients. This helps a subscriber ensure that the correct recipient is selected when he or she addresses a voice mail message. The inclusion of the remote location information in the confirmation (if applicable) helps to ensure that the message is sent to the correct location. | "Revisiting the Installation Configuration" on page 20 and "Configuring Peer Messaging Gateways" on page 24 |
| **Real-time notification of network availability** | Real-time notification of Cisco Unity Express 3.1 and later versions availability. | "Viewing Network Status" on page 53 |



# Overview of Cisco Unified Messaging Gateway 1.0

**Last updated: April 13, 2010**



## Introduction

Cisco Unified Messaging Gateway (Cisco UMG) delivers the end-to-end message networking functionality required by larger distributed enterprises seamlessly migrating to Cisco's IPT solution. The majority of larger distributed enterprises consist of various legacy voice messaging products that do not support open standards. The Cisco UMG solution fulfills a gateway function for these networks, providing a method of intelligently routing messages, exchanging subscriber and directory information, and providing interoperability within a messaging network. It acts as a central hub for distributed messaging deployments, specifically:

- Cisco Unity Express
- Cisco Unity 4.2 and later versions for Microsoft Exchange only
- Avaya Interchange 5.4

Cisco UMG enables the messaging network to scale as required for the largest of implementations and simplifies configuration of all the endpoints. In particular, it enables Cisco Unity Express 3.1 and later versions to autoregister with the system.

Cisco UMG is an application that resides on an enhanced network module (NME). The module plugs into a host Cisco router running Cisco IOS software.

The Cisco Unified Messaging Gateway enhanced network module (NME-Cisco UMG family of devices) is available in two models (see Table 2 on page 6). All models ship from the factory with the software preinstalled.

*Table 2 Cisco UMG Enhanced Network Modules Models and Capacities*

| Model | Number of Cisco Unity Express Endpoints Supported per Cisco UMG network module | Number of Subscribers on Cisco Unity Express Endpoints Supported per System of 20 Cisco UMGs |
|---|---|---|
| NME-UMG | 250 maximum | 125,000 maximum |
| NME-UMG-EC | 1000 maximum | 500,000 maximum |

A system of 20 Cisco UMGs comprises both primary and secondary messaging gateways, therefore such a system supports 500,000 subscribers rather than 1,000,000.

**Caution** Do not combine the two types of network module into a single system. Because the messaging gateways must be synchronized, each one must accommodate the same size of data dump.

Guidelines and procedures for installing Cisco UMG are described in the *Cisco Unified Messaging Gateway 1.0 Installation Guide*. The individual CLI commands are described in the *Cisco Unified Messaging Gateway 1.0 Command Reference.*

# Functional Outline

A Cisco UMG system can consist of up to 20 fully meshed messaging gateways, all of the same type. NME-UMG supports up to 250 endpoints; a system composed of 20 NME-UMGs supports at least 12,500 subscribers. NME-UMG-EC supports up to 1000 endpoints; a system composed of 20 NME-UMG-ECs supports up to 500,000 subscribers.

Do not mix the two types of network module in one system. In a Cisco UMG system, you can have either all NME-UMGs or all NME-UMG-ECs.

If your endpoints are Cisco Unity Express 3.1 and later versions, you can set up your system so that your endpoints (nodes) autoregister with messaging gateways. If you have other types of endpoints, including Cisco Unity Express 3.0 or earlier versions, you must manually provision them from messaging gateways.

**Note** Only endpoints running Cisco Unity Express 3.1 and later versions can autoregister; all other types of endpoints must be manually provisioned (see "Manual Provisioning of Cisco Unity and Avaya Interchange Endpoints" on page 7).

### Autoregistration

The purpose of autoregistration between Cisco UMG and Cisco Unity Express 3.1 and later versions is to facilitate scaling your messaging network while ensuring that messages can only be exchanged by trusted peers. Autoregistration is the means by which a messaging gateway can automatically "discover" legitimate endpoints. The messaging gateway authorizes such endpoints by validating shared secret information. Autoregistration also enables messaging gateways to learn about endpoint properties through directory exchange.

For a more detailed description of the autoregistration process, see "Overview of the Autoregistration Process" on page 91.

### Manual Provisioning of Cisco Unity and Avaya Interchange Endpoints

Endpoints running Cisco Unity Express 3.0 or earlier versions, Cisco Unity, and Avaya Interchange cannot autoregister, therefore they must be manually provisioned from Cisco UMG. This serves the same purpose as the registration described previously, ensuring that information is only exchanged between trusted peers. Also, because these endpoint types do not support automatic directory exchange, you must configure the directory information for them on the messaging gateway that manages them.

**Note** Registered endpoints stay in the database. When an endpoint registers with Cisco UMG, it is assigned a guide number that it uses to identify itself to the messaging gateway on subsequent registrations. If an endpoint tries to register without that guide number or with a different messaging gateway, the registration is rejected as a duplicate location. If necessary, you can clear or delete the endpoint (see "Deleting or Clearing Endpoints" on page 75.

### Directory Exchange Between Endpoints And Messaging Gateways

After endpoints are registered with or provisioned to a messaging gateway, this message gateway will propagate the endpoints' information to the rest of the network of Cisco UMGs.

Endpoints can:

- Exchange messages with the messaging gateway with which they are registered
- Retrieve remote subscriber information from that messaging gateway

**Note** Endpoints of the type Cisco Unity Express 3.0 or earlier versions cannot perform autoregistration and directory exchange with Cisco UMG. Neither can Cisco Unity or Avaya Interchange.

### Remote Lookup Function

Subscribers can use the remote lookup function to search for a subscriber. The subscriber thus has the ability to:

- Decide whether the remote mailbox exists on an autoregistered endpoint running Cisco Unity Express 3.1 and later versions (this directory exchange facility is not yet supported for other types of endpoint)
- Search the global directory, for example, when the message sender does not know the recipient's number.

  **Note** In the global directory, the subscriber will not find search results already delivered by the local directory. This feature serves to prevent the global search results from being flooded by results already obtained.

- Retrieve the spoken name of the remote subscriber. By default, the spoken name is carried in all directory exchange messages.

  **Note** This feature can be turned off in cases where network bandwidth, performance, and database storage might be problematic.

# Managing a Network of Cisco UMGs

Each messaging gateway is configured to recognize its peers. After endpoints are registered with or provisioned to a messaging gateway, this messaging gateway will propagate the endpoints' information to the rest of the network of Cisco UMGs.

Cisco UMG uses the primary/secondary model to provide failover support. Each Cisco Unity Express endpoints identifies primary and secondary messaging gateway through its local configuration and autoregisters with both messaging gateways. For Cisco Unity, a DNS server is required for failover support, meaning that the messaging gateway domain name will be mapped to two IP addresses on DNS: primary messaging gateway and secondary messaging gateway. Avaya Interchange does not support such failover provisions.

In the case of a firewall, a firewall pin hole must be opened to allow TCP connections between two different nodes (such as between an endpoint and Cisco UMG or between messaging gateways, and so on).

# Administration Interfaces

Cisco UMG has a single administration interface, the command-line interface (CLI). This is a text-based interface accessed through a Telnet session to the router hosting Cisco UMG. Those familiar with Cisco IOS command structure and routers will see similarities.

The Cisco UMG commands are structured much like the Cisco IOS CLI commands. However, the Cisco UMG CLI commands do not affect Cisco IOS configurations. After you log in to Cisco UMG, the command environment is no longer the Cisco IOS environment.

See "Entering and Exiting the Command Environment" on page 15 for the instructions to enter the Cisco UMG CLI environment.

The CLI is accessible from a PC or server anywhere in the IP network.

# Additional References

The following sections provide references related to Cisco Unified Messaging Gateway.

## Documents Related to Cisco Unified Messaging Gateway

| Related Topic | Document Title |
|---|---|
| Cisco UMG 1.0 Installation | *Cisco Unified Messaging Gateway 1.0 Installation Guide* |
| Cisco UMG 1.0 Command Reference | *Cisco Unified Messaging Gateway 1.0 Command Reference Guide* |
| Late-breaking information about Cisco Unified Messaging Gateway 1.0 | *Cisco Unified Messaging Gateway 1.0 Release Notes* |
| Cisco network modules hardware installation | *Cisco Network Modules Hardware Installation Guide* |
| Cisco Unity Express | Cisco Unity Express: complete documentation set at http://www.cisco.com/en/US/products/sw/voicesw/ps5520/tsd_products_support_series_home.html |

| Related Topic | Document Title |
|---|---|
| Cisco Unity | Cisco Unity: complete documentation set at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/tsd_products_support_series_home.html |
| Cisco hardware platforms | • *Cisco 2800 Series Hardware Installation Guide*<br>• *Cisco 2800 Series Hardware Configuration Notes*<br>• *Voice Features on Cisco 2800 Series Routers*<br>• *Cisco 3800 Series Hardware Installation*<br>• *Cisco 3800 Series Software Configuration* |

## RFCs

| RFCs | Title |
|---|---|
| 1869 | *SMTP Service Extensions* |
| 1893 | *Enhanced Mail System Status Codes* |
| 2045 | *Multipurpose Internet Mail Extensions Part One: Format of Internet Message Bodies, RFC* |
| 2421 | *Voice Profile for Internet Mail - Version 2* |
| 2426 | *vCard MIME Directory Profile* |
| 2617 | *HTTP Authentication: Basic and Digest Access Authentication* |
| 2821 | *Simple Mail Transfer Protocol* |
| 2833 | *RTP Payloads for DTMF Digits, Telephony Tones and Telephony Signals* |
| 3261 | *SIP: Session Initiation Protocol* |
| 3501 | *Internet Message Access Protocol - Version 4rev1* |

# Obtaining Documentation and Submitting a Service Request

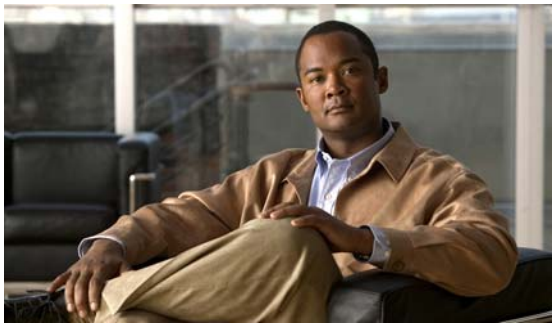
For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

# Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.<br><br>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and (RSS) Feeds.<br><br>Access to most tools on the Cisco Support website requires a Cisco.com username and password. | http://www.cisco.com/techsupport |



# Configuring Cisco Unified Messaging Gateway

**Last updated: April 13, 2010**

This chapter provides a sequential overview of the tasks described in this guide. They are grouped into categories as follows:



Enter the command environment either by bridging the access from the router or by telnet, as described in "Entering and Exiting the Command Environment" on page 15. Proceed with the tasks described below, in sequence.

**Note** Before you start configuring your system, verify its status to ensure that your installation is correct. See "Verifying System Status" in the *Cisco Unified Messaging Gateway 1.0 Installation Guide*.

**Note** Copy your configurations frequently to the startup-config. Almost all the configurations described in this guide are saved to the running-config. However, if you must reboot, only the configurations saved to the startup-config will be used. If you delete from the running-config a configuration that you have already copied to the startup-config, the configuration reappears when you reboot.

Before you begin the tasks listed in Table 3, map out your solution topology so that each messaging gateway and each endpoint has a unique location ID. This is a numeric string of up to ten digits. System Distribution Lists (SDLs) require list numbers that are distinct from subscriber numbers, because the SDL numbers are those the authorized senders dial to access the SDLs.

# Task Set 1: Initial Configuration

*Table 3 Initial Configuration Tasks*

| Task and Procedure Location | Description |
|---|---|
| Revisiting the Installation Configuration, page 20 | Use these procedures to change the configurations that you made during installation. |
| Setting Backup Parameters, page 22 | Use these procedures to enable backup and thus restoring. |
| Configuring Peer Messaging Gateways, page 24 | Use this procedure to configure peers on each messaging gateway. |
| Message Handling, page 26 | Use these procedures to set a default destination for undeliverable messages and specify when the system sends delayed delivery receipts (DDRs) and non-delivery receipts (NDRs). |
| Configuring Endpoint Autoregistration Support, page 28 | Use these configurations to enable Cisco Unity Express 3.1 and later versions to autoregister with Cisco UMG. |
| Provisioning Endpoints Manually, page 31 | Use these configurations to enable endpoints of these types to register with Cisco UMG:<br>• Cisco Unity Express 3.0 or earlier versions<br>• Cisco Unity<br>• Avaya Interchange |
| Setting Up NAT Entries, page 36 | Use these procedures if you have NAT devices between messaging gateways and/or endpoints. On Cisco UMG you must configure the access information for the NAT device in front of the destination. |
| Configuring NTP Servers, page 38 | Use this procedure to configure NTP servers. The system uses a DNS server to resolve the hostname to an IP address and stores the IP address as an NTP server. |
| Setting the Time Zone, page 42 | If your messaging gateways are located in different time zones, use this procedure to set the time zone for each one. |
| Configuring Logging Operations, page 43 | This section describes the specifications necessary to set up logging. |

# Task Set 2: Backing Up and Restoring

*Table 4 Backing Up and Restoring*

| Task and Procedure Location | Description |
|---|---|
| Backing Up and Restoring Data, page 45 | Backup is allowed only when the system is in offline mode. By default, both configuration data and the dynamically captured data are backed up; however, they are not backed up automatically. |

# Task Set 3: Ongoing Maintenance Tasks

*Table 5 Ongoing Maintenance Tasks*

| Task and Procedure Location | Description |
|---|---|
| Viewing Network Status, page 53 | Use to verify the status of peer messaging gateways and endpoints |
| Locating and Viewing Individual Mailbox Details, page 54. | Use to locate an individual mailbox and view its details. |
| Displaying Management Data Activity, page 56 | Use to display management data activity. |
| Checking Hard Disk Memory Wear Activity, page 56 | Use to track the use and wear of the hard disk memory. |
| Viewing System Activity Messages, page 57 | Use to capture messages that describe activities in the system. |
| Checking Log and Trace Files, page 57 | Use to check the log and trace files on the hard disk. |

# Task Set 4: As-Needed Tasks

*Table 6 As-Needed Tasks*

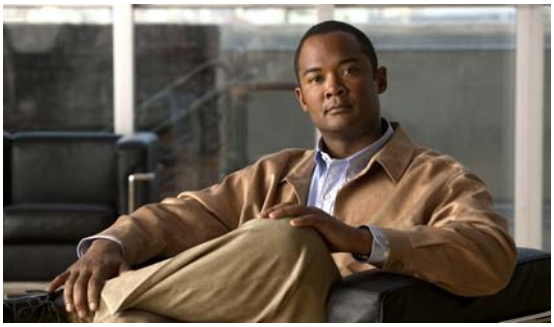
| Task and Procedure Location | Description |
|---|---|
| Copying Configurations, page 59 | Use to copy the startup configuration and running configuration to and from the hard disk on the Cisco UMG module. |
| Restoring Factory Default Values, page 63 | Use to restore the factory default values for the entire system. |
| Going Offline, Reloading, Rebooting, Shutting Down, and Going Back Online, page 63 | Use for going offline, reloading the blade, shutting it down, and going back online. |
| Forcing Data Convergence, page 66 | Use to enable the current configuring messaging gateway to obtain or provide updates or directory exchanges. |
| Managing System Distribution Lists, page 67 | Use to manage SDLs. |
| Managing System Broadcasts, page 71 | Use to manage System Broadcast Messages (SBMs). |
| Deleting Peer Messaging Gateways, page 73 | Use to clear data relating to a peer messaging gateway. |
| Deleting or Clearing Endpoints, page 75 | Use to clear data relating to an endpoint. |
| Blocking Endpoint Registration, page 76 | Use to prevent endpoints from autoregistering. |
| Checking Endpoint Mailboxes, page 78 | Use to view the details relating to a mailbox. |

# Task Set 5: Troubleshooting

*Table 7 Troubleshooting*

| Task and Procedure Location | Description |
|---|---|
| General Troubleshooting Guidelines, page 79 | Use when troubleshooting |
| System Reports, page 87 | Use to find out which system reports Cisco UMG provides. |
| Hardware and Software, page 80 | Use to identify a problem and its solution. |
| Saving and Viewing Log Files, page 86 | Use to help identify problems and recommended actions. |
| Saving Configuration Changes, page 85 | Use to help identify problems and recommended actions. |
| Message Transmission, page 83 | Use to change message translation rules with the help of Cisco Support. |
| Trace Commands, page 87 | Use to perform tracing operations. |
| Logging Commands in Cisco UMG EXEC Mode, page 82 | Use to perform logging operations. |
| Logging Commands in Cisco UMG Configuration Mode, page 82 | Use to perform logging operations. |
| Show Commands, page 86 | Use to display configurations. |

**Tip** Bookmark the Cisco Unified Messaging Gateway documentation for easy access to all the documents. Print and have available the documentation for these Ongoing and As-Needed tasks.



# Entering and Exiting the Command Environment

**Last updated: April 13, 2010**

This chapter describes the procedures for entering and exiting the Cisco Unified Messaging Gateway command environment, where Cisco UMG configuration commands are executed. The following sections describe these procedures:



## EXEC and Configuration Modes

Cisco UMG uses the network module's CLI, which you access through the host-router console. The network module CLI is similar to the router CLI:

### Similarities

Standard Cisco IOS navigation and command-completion conventions apply (for example, **?** lists options, **TAB** completes a command, and **|** directs **show** command output).

### Differences

Standard command names and options do *not* necessarily apply. A notable example is the command for accessing global configuration mode: the Cisco IOS command is **configure terminal**; the network module command is **config terminal or config t**.

Cisco UMG employs a last-one-wins rule. For example, if George and Frank both try to set the IP address for the same entity at the same time, the system starts and completes one operation before it starts the next. The last IP address set is the final result.

The Cisco UMG command modes, privileged EXEC, configuration, registration configuration, list configuration, endpoint configuration, and NAT configuration operate similarly to the EXEC and configuration modes in the Cisco IOS CLI.

After you enter configuration mode, all the CLI commands can be used in the **no** form, for example, **no network messaging gateway location-id { hostname | ip-address }**. This command deletes the specified peer messaging gateway.

# Entering the Command Environment

After the Cisco UMG network module is installed, IP connectivity with it established, and the software active, use this procedure to enter the command environment.

## Prerequisites

The following information is required to enter the Cisco UMG command environment:

- IP address of the router that contains the Cisco UMG module
- Username and password to log in to the router
- Slot in the router where the Cisco UMG network module resides
- Port through which the router communicates with Cisco UMG

### SUMMARY STEPS

1. Open a telnet session.
2. **telnet** *ip-address*
3. Enter the username and password of the router.
4. **service-module integrated-Service-Engine** *slot/port* **session**
5. (Optional) **enable**

### DETAILED STEPS

| | Command or Action | Explanation |
|---|---|---|
| **Step 1** | Open a telnet session. | Use a DOS window, a secure shell, or a software emulation tool such as Reflection. |
| **Step 2** | **telnet** *ip-address*<br><br>**Example:**<br>`C:\>telnet 192.0.2.22` | Specifies the IP address of Cisco UMG's host router. |
| **Step 3** | `Username:`<br>`Password:` | Enter your username and password for the router. |

| | Command or Action | Explanation |
|---|---|---|
| **Step 4** | **service-module integrated-Service-Engine** *slot/port* **session**<br><br>**Example:**<br>`Router# service-module integrated-Service-Engine 1/0 session` | Enters the Cisco UMG command environment using the module located in *slot* and *port*. The first time you do this, the prompt changes to "se" with the IP address of the Cisco UMG module. After that, the prompt is the hostname you give to the module.<br><br>If entering *ip-address slot/port* elicits the response "Connection refused by remote host" enter the command **service-module integrated Service-Engine** *slot/port* **session clear** and retry this step. |
| **Step 5** | **enable**<br><br>**Example:**<br>`se-10-0-0-0# enable` | Enters Cisco UMG EXEC mode. You are ready to begin configuration. |

# Exiting the Command Environment

To leave the Cisco UMG command environment and return to the router command environment, in Cisco UMG EXEC mode enter the **exit** command once to exit EXEC mode, and again to exit the application.

The following example illustrates the exit procedure:

```
se-10-0-0-0# exit
se-10-0-0-0# exit
router-prompt#
```

# Initial Configuration Tasks

**Last updated: April 13, 2010**

This chapter describes how to set up your Cisco Unified Messaging Gateway system after you have installed it.

You must configure each messaging gateway in your system. If your endpoints are Cisco Unity Express 3.1 and later versions, you only need to set up autoregistration on one messaging gateway.

With Cisco Unity Express 3.0 or earlier versions, Cisco Unity, and Avaya Interchange endpoints, you must manually provision each one on the messaging gateway associated with it. The messaging gateway on which you manually provision an endpoint becomes that endpoint's primary messaging gateway. You can change the configuration of these types of endpoints only from their primary messaging gateway.

The chapter contains the following sections:



For a brief overview of how the system works, see the "Functional Outline" on page 6.

The "Monitoring the Cisco Unified Messaging Gateway System" chapter covers monitoring tasks, while the "Maintaining the Cisco Unified Messaging Gateway System" chapter covers System Distribution Lists (SDLs) and System Broadcast Messages (SBMs) and also deleting various entities.

Cisco UMG is configured entirely using the command-line interface (CLI). You enter some commands in EXEC mode and others in configuration mode, and still others in submodes. The instructions for each of the tasks cover entering the mode to be used.

For instructions on entering and exiting command modes, see the "Entering and Exiting the Command Environment" chapter.

# Revisiting the Installation Configuration

If you used the interactive post-installation wizard, you will have completed these configurations. If you did not choose this method of installation or if you want to change any of the configurations, use these instructions to:

- Specify the messaging gateway hostname
- Specify the messaging gateway location ID
- Specify the messaging gateway domain name
- (Optional) Specify DNS servers if necessary
- (Optional) Spoken name capability—Enabling this functionality permits a message sender's spoken name to be played at the beginning of the received message. Disabling spoken name capability saves bandwidth. Although you can set this differently on different messaging gateways, for best performance, use the same setting for this on all messaging gateways throughout your system.

  **Note** To disable spoken-name capability, use the **no** form of this command.

- Verify settings are correct by using appropriate **show** commands

## Prerequisites

The following information is required to configure Cisco UMG:

- Hostname
- Location ID, unique within the solution network
- Name of the messaging gateway's domain
- IP addresses of the DNS server(s) the messaging gateway will use (if applicable)

**Note** A DNS server is only necessary if you have Cisco Unity endpoints, in which case it is essential to provide failover support for these endpoints. You can use a maximum of four DNS servers.

### SUMMARY STEPS

1. **config t**
2. **network local messaging-gateway** *location-id*
3. **hostname** *hostname*
4. **ip { domain-name** *domain-name* **| name-server** *name-server* }
5. **ip { domain-name** *domain-name* **| name-server** *name-server* }
6. **spoken-name enable**
7. **end**
8. **show hosts**
9. **show messaging-gateway [** *location-id* **]**
10. **show spoken-name**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **config t**<br><br>**Example:**<br>`se-10-0-0# config t` | Enters configuration mode. |
| **Step 2** | **network local messaging-gateway** *location-id*<br><br>**Example:**<br>`se-10-0-0(config)# network local messaging-gateway 50000` | Specifies the current configuring messaging gateway's location ID. |
| **Step 3** | **hostname** *hostname*<br><br>**Example:**<br>`se-10-0-0(config)# hostname umg-1` | Specifies the messaging gateway's hostname. |
| **Step 4** | **ip { domain-name** *domain-name* \| **name-server** *name-server* }<br><br>**Example:**<br>`umg-1(config)# ip domain-name mycompany.com` | Specifies the domain name (not including the hostname) or the DNS server(s) (max. 4) for the current configuring messaging gateway. |
| **Step 5** | **ip { domain-name** *domain-name* \| **name-server** *name-server* }<br><br>**Example:**<br>`umg-1(config)# ip name-server 192.0.2.24` | Specifies the domain name (not including the hostname) or the DNS server(s) (max. 4) for the current configuring messaging gateway. |
| **Step 6** | **spoken-name enable**<br><br>**Example:**<br>`umg-1(config)# spoken-name enable` | Enables spoken name support on the current configuring messaging gateway. For best performance, this setting should be the same on all messaging gateways in the system. |
| **Step 7** | **end**<br><br>**Example:**<br>`umg-1(config)# end` | Exits configuration mode. |
| **Step 8** | **show hosts**<br><br>**Example:**<br>`umg-1# show hosts` | Displays the hostname and domain name. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 9** | **show messaging-gateway [** *location-id* **]**<br><br>**Example:**<br>`umg-1# show messaging-gateway` | Displays the location ID and hostname of any peer messaging gateways that have been configured, whether NAT is enabled for any of them, and the location ID of the current configuring messaging gateway. If a location ID other than the current configuring messaging gateway is specified, displays the named details for the specified messaging gateway. |
| **Step 10** | **show spoken-name**<br><br>**Example:**<br>`umg-1# show spoken-name` | Indicates whether spoken name support is enabled. |

## Examples

The following output illustrates the use of these commands.

```
se-10-0-0# config t
se-10-0-0(config)# network local messaging-gateway 50000
se-10-0-0(config)# hostname umg-1
umg-1(config)# ip domain-name mycompany.com
umg-1(config)# ip name-server 192.0.2.24
umg-1(config)# spoken-name enable
umg-1(config)# end
umg-1# show hosts
Hostname:      umg-1
Domain:        mycompany.com
umg-1# show messaging-gateway
LocationID     Hostname                              NAT
-------------------------------------------------------------
5              sj.mycompany.com                      disabled
55             sf.mycompany.com                      disabled
555            ny.mycompany.com                      disabled

Local Gateway ID: 50000
umg-1# show spoken-name
Spoken name is enabled.
umg-1#
```

# Setting Backup Parameters

Cisco UMG backup and restore functions use an FTP server to store and retrieve data. The backup function copies the files from Cisco UMG to the FTP server and the restore function copies the files from the FTP server to Cisco UMG. The FTP server can reside anywhere in the network as long as the backup and restore functions can access it with an IP address or hostname.

All Cisco UMG backup files are stored on the specified server. You can copy the backup files to other locations or servers, if necessary.

The backup parameters specify the FTP server to use for storing Cisco UMG backup files and the number of backups that are stored before the system overwrites the oldest one.

**Note** Cisco UMG automatically assigns an ID to each successful backup. To find out what ID has been assigned to your backup, use the **show backup history** command. For more information, see "Restoring Files" on page 49.

To backup or restore files, see the "Backing Up and Restoring Data" chapter.

# Prerequisites

- Verify that the backup server is configured.
- Verify that an FTP administrator or other user who can log in to the FTP server has full permission on the FTP server, such as read, write, overwrite, create, and delete permissions for files and directories.
- FTP server URL
- Username and password of the FTP server login
- Number of revisions to save before the oldest backup is overwritten

## SUMMARY STEPS

1. **config t**
2. **backup server url** *backup-ftp-url* **username** *backup-ftp-usrname* **password** *backup-ftp-password*
3. **backup revisions number** *number*
4. **end**
5. **show backup**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **config t**<br><br>umg-1# config t | Enters configuration mode. |
| **Step 2** | **backup server url** *ftp-url* **username** *ftp-username* **password** *ftp-password*} | Sets the backup parameters.<br>**Note** The backup server must be configured before the backup revisions can be configured.<br>• **server url**—The *ftp-url* value is the URL to the network FTP server where the backup files will be stored.<br>• The *ftp-username* and *ftp-password* values are the username and password for the network FTP server.<br>In the example, **main** is the hostname of the FTP server and **backups** is the directory where backup files are stored. |
| | **Example:**<br>umg-1(config)# **backup server url ftp://main/backups username "admin" password "wxyz"**<br><br>umg-1(config)# **backup server url ftp://192.0.2.15/backups username "admin" password "wxyz"** | |

| | Command or Action | Purpose |
|---|---|---|
| Step 3 | **backup revisions** *number*<br><br>**Example:**<br>`umg-1(config)# backup revisions 5` | Sets the number of backup files that will be stored. When this number is reached, the system deletes the oldest stored file. |
| Step 4 | **exit**<br><br>**Example:**<br>`umg-1(config)# exit` | Exits configuration mode. |
| Step 5 | **show backup**<br><br>**Example:**<br>`umg-1# show backup` | Displays the backup server configuration information, including the FTP server URL and the maximum number of backup files available. |

# Examples

The following example configures a backup server and displays the **show backup** output:

```
umg-1# config t
umg-1(config)# backup revisions 5
umg-1(config)# backup server url ftp://main/umg-1backups username "admin" password "wxyz"
umg-1#(config)# end
umg-1# show backup
Server URL:                             ftp://branch/umg-1backups
User Account on Server:                 backupadmin
Security Protected:                     no
Security Enforced:                      no
Number of Backups to Retain:            5
umg-1#
```

# Configuring Peer Messaging Gateways

You can configure multiple peer Cisco UMGs. Location IDs for peer messaging gateways must be unique throughout the solution network.

Not only must you configure peers on each messaging gateway, you must also configure each peer as a messaging gateway. For this, use all the procedures in this chapter.

To delete a peer messaging gateway, see "Deleting Peer Messaging Gateways" on page 73.

**Note** The following commands do not validate the hostname or IP address of the peer messaging gateway.

## Prerequisites

The following information is required to configure a peer Cisco UMG:

- A location ID for the peer messaging gateway that is unique throughout the system.
- A hostname.

## SUMMARY STEPS

1. **config t**
2. **network messaging-gateway** *location-id* { *hostname* | *ip-address* }
3. **end**
4. **show messaging-gateway** [*location-id* ]
5. **show messaging-gateway** [*location-id* ]

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **config t**<br><br>**Example:**<br>`umg-1# config t` | Enters configuration mode |
| **Step 2** | **network messaging-gateway** *location-id* **{** *hostname* **\|** *ip-address* **}**<br><br>**Example:**<br>`umg-1(config)# network messaging-gateway 5 sj.mycompany.com` | Configures a peer messaging gateway. The hostname can be in the form sj.mycompany.com or it can be an IP address. |
| **Step 3** | **end**<br><br>**Example:**<br>`umg-1(config)# end` | Exits configuration mode. |
| **Step 4** | **show messaging-gateway** [ *location-id* ]<br><br>**Example:**<br>`umg-1# show messaging-gateway` | Displays the location ID and hostname of any peer messaging gateways that have been configured, whether NAT is enabled for any of them, and the location ID of the current configuring messaging gateway. If a location ID other than the current configuring messaging gateway is specified, displays the named details for the specified messaging gateway. |
| **Step 5** | **show messaging-gateway** [ *location-id* ]<br><br>**Example:**<br>`umg-1# show messaging-gateway 5` | Displays the location ID and hostname of any peer messaging gateways that have been configured, whether NAT is enabled for any of them, and the location ID of the current configuring messaging gateway. If a location ID other than the current configuring messaging gateway is specified, displays the named details for the specified messaging gateway. |

## Examples

The following output illustrates the use of these commands.

```
umg-1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
umg-1(config)# network messaging-gateway 5 sj.mycompany.com
umg-1(config)# end
umg-1# show messaging-gateway
LocationID     Hostname                              NAT
-------------------------------------------------------------
5              sj.mycompany.com                      disabled
55             sf.mycompany.com                      disabled
555            ny.mycompany.com                      disabled

Local Gateway ID: 51000
umg-1# show messaging-gateway 5
LocationID:    5
Hostname:      sj.mycompany.com
NAT:           disabled

umg-1#
```

# Message Handling

## Default Destination

You can set a default destination (‘network default-route’) for undeliverable messages; the destination can be either a messaging gateway or an endpoint.

## Notice of Delayed Delivery or Non-delivery

If a message is not delivered within one hour of being sent, by default Cisco UMG sends a delayed-delivery receipt (DDR) to the message-sender and a non-delivery receipt (NDR) after six hours. These settings are system-wide, they cannot be applied to individual endpoints.

Changing the defaults is optional. If you do not make the settings described in the following procedure, the system uses the defaults.

## Prerequisites

The following information is required to configure the default destination for unroutable messages:

- The location ID of the endpoint or the messaging gateway to which unroutable messages are to be sent.

The following information is required to change the DDR and NDR settings:

- Delay in hours to be substituted for the current settings (defaults are DDR: 1 hour, NDR: 6 hours).

## SUMMARY STEPS

1. **config t**
2. **network default-route** *location-id*
3. **ddr timeout** *0-24*
4. **ndr timeout** *1-48*
5. **end**
6. **show network default-route**
7. **show ddr timeout**
8. **show ndr timeout**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **config t**<br><br>**Example:**<br>`umg-1# config t` | Enters configuration mode. |
| **Step 2** | **network default-route** *location-id*<br><br>**Example:**<br>`umg-1(config)# network default-route 987654` | Sets the default destination for undeliverable messages. |
| **Step 3** | **ddr timeout** <*0-24*><br><br>**Example:**<br>`umg-1(config)# ddr timeout 2` | Sets the amount of time (in hours) before the system generates a DDR. Range: 1-24 hours. Set 0 to disable this feature. Default: 1 hour. |
| **Step 4** | **ndr timeout** <*1-48*><br><br>**Example:**<br>`umg-1(config)# ndr timeout 12` | Sets the amount of time (in hours) before the system generates an NDR. Range: 1-48 hours. Default: 6 hours. |
| **Step 5** | **end**<br><br>**Example:**<br>`umg-1(config)# end` | Exits configuration mode. |
| **Step 6** | `show ddr timeout`<br><br>**Example:**<br>`umg-1# show ddr timeout` | Displays the delay before the system generates a DDR. |
| **Step 7** | `show ndr timeout`<br><br>**Example:**<br>`umg-1# show ndr timeout` | Displays the delay before the system generates an NDR. |

## Examples

The following example illustrates default destination for undeliverable messages being set to the device with the location ID 51000, and the DDR and NDR timeouts being set for the system.

```
umg-1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
umg-1(config)# network default-route 51000
umg-1(config)# ddr timeout 2
umg-1(config)# ndr timeout 12
umg-1(config)# end
umg-1# show network default-route
Default route is location 51000.

umg-1# show ddr timeout
Timeout window for DDR messages is 2 hours.

umg-1# show ndr timeout
Timeout window for NDR messages is 12 hours.

umg-1#
```

# Configuring Endpoint Autoregistration Support

For endpoints that are to autoregister with Cisco UMG, you must configure registration, connection, and authentication parameters.

You can configure multiple username/password sets on the same messaging gateway.

**Note** Only Cisco Unity Express 3.1 and later versions support autoregistration.

The endpoints themselves must be configured to present the corresponding information in a registration request.

The default registration period expires after 1440 minutes. After that time, any new configurations such as username and password take effect.

For an overview of the relevant Cisco Unity Express configuration, see "Appendix A: Cisco Unity Express Endpoint Autoregistration to Cisco Unified Messaging Gateway 1.0" on page 91.

In the system logic, autoregistration is implicitly allowed for all endpoints, therefore to prevent autoregistration you must use the **block** command described in this section or in "Blocking Endpoint Registration" on page 76.

To clear the data associated with an autoregistered endpoint, see "Deleting or Clearing Endpoints" on page 75.

## Prerequisites

The following information is required to configure endpoint autoregistration parameters on Cisco UMG.

- Username and password for endpoints to present to Cisco UMG at registration
- (Optional) Location IDs for endpoints that you want to prevent from autoregistering
- (Optional) Registration expiration period, in minutes

## SUMMARY STEPS

1. **config t**
2. **registration**
3. **username** *username* **password** {**text** | **encrypted** } *password*
4. **expiration** *integer*
5. **block location-id** *location-id*
6. **end**
7. **end**
8. **show run** [ **paged** | | [**begin** *word* | **exclude** *word* | **include** *word* | **page** ]
9. **write [ erase | memory | terminal ]**
10. **show start** [ **paged** | | [**begin** *word* | **exclude** *word* | **include** *word* | **page** ]
11. **show registration** {**block** | **status** | **users** }

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **config t**<br><br>**Example:**<br>umg-1# config t | Enters configuration mode. |
| **Step 2** | **registration**<br><br>**Example:**<br>umg-1(config)# registration | Enters registration configuration mode. |
| **Step 3** | **username** *username* **password { text \| encrypted }** *password*<br><br>**Example:Example:**<br>umg-1(config-reg)# username bob password text cue31 | Sets username and password. |
| **Step 4** | **expiration** *integer*<br><br>**Example:**<br>umg-1(config-reg)# expiration 2000 | (Optional) Sets the length of time (in minutes) after which autoregistration expires. |
| **Step 5** | **block location-id** *location-id*<br><br>**Example:Example:**<br>umg-1(config-reg)# block location-id 29 | Prevents the specified endpoint from autoregistering. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **end**<br><br>**Example:**<br>`umg-1(config-reg)# end` | Exits registration configuration mode. |
| **Step 7** | **end**<br><br>**Example:**<br>`umg-1(config)# end` | Exits configuration mode. |
| **Step 8** | **show run [ paged \| \| [begin** *word* **\| exclude** *word* **\| include** *word* **\| page ]**<br><br>**Example:**<br>`umg-1# show run \| inc username` | Displays the running configuration. |
| **Step 9** | **write [erase \| memory \| terminal ]**<br><br>**Example:**<br>`umg-1# write memory` | Writes the running configuration to memory or terminal or<br>• Erases NV memory<br>• Writes to NV memory<br>• Writes to terminal. |
| **Step 10** | **show start [ paged \| \| [begin** *word* **\| exclude** *word* **\| include** *word* **\| page ]**<br><br>**Example:**<br>`umg-1 show start \| inc username` | Displays the startup configuration. |
| **Step 11** | **show registration { block \| status \| users }**<br><br>**Example:**<br>`umg-1# show registration block` | Displays endpoint registration status. |

## Examples

The following example shows an expiration being set for all autoregistered endpoints. A block is set, then a username and password. Finally, the results of these operations are displayed. Note that the expiration is not displayed, because the **no expiration** command caused the default to be set.

```
umg-1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
umg-1(config)# registration
umg-1(config-reg)# expiration 20000
Currently registered endpoint expiration will be unaffected.
umg-1(config-reg)# block location-id 33
umg-1(config-reg)# username bob password text cue31
umg-1(config-reg)# end
umg-1(config)# end
umg-1 show run | inc username
 username bob password text cue31
```

```
umg-1# write memory
umg-1 show start | inc username
 username bob password text cue31
umg-1# show registration block
UMG registration block list :
        location-id 33
se-10-1-12-95# show registration status
Endpoint registration stats :
        Auto-registered : 1
        Offline : 10
        Total number : 11

Auto-registered endpoint :
         Loc. 40000 : cue, registered at 19-Aug-07 17:02:31:212

Offline auto-registered endpoint :
         Loc. 40 : cue, deregistered/unreachable since 17-Aug-07 16:56:45:177
         Loc. 41 : cue, deregistered/unreachable since 17-Aug-07 16:56:45:177
         Loc. 42 : cue, deregistered/unreachable since 17-Aug-07 16:56:32:169
         Loc. 43 : cue, deregistered/unreachable since 17-Aug-07 16:56:45:177
         Loc. 44 : cue, deregistered/unreachable since 17-Aug-07 16:56:45:177
         Loc. 45 : cue, deregistered/unreachable since 17-Aug-07 16:56:45:177
         Loc. 46 : cue, deregistered/unreachable since 17-Aug-07 16:56:45:177
         Loc. 47 : cue, deregistered/unreachable since 17-Aug-07 16:56:45:177
         Loc. 48 : cue, deregistered/unreachable since 17-Aug-07 16:56:45:177
umg-1#
```

# Provisioning Endpoints Manually

You must manually provision Cisco Unity and Avaya Interchange endpoints to Cisco UMG. Endpoints of the type Cisco Unity Express 3.0 or earlier versions must also be manually provisioned.

The configuring Cisco UMG automatically becomes the primary messaging gateway for the endpoint being provisioned.

It is most efficient if you group your endpoints by type (Cisco Unity, Cisco Unity Express, Avaya Interchange) before provisioning them, because each type has one or two parameters that are different from those required for other types.

**Note** For Cisco Unity endpoints, to provide failover support you need at least one DNS server (maximum 4) so that you can map the Cisco UMG domain name to two IP addresses on it (them): primary messaging gateway and secondary messaging gateway.

When you configure a domain for an endpoint, Cisco UMG does an MX lookup on the domain provided and uses those host addresses.

If you have multiple endpoints with the same prefix, you must use the **number-only** addendum to the **prefix** command to specify the range of extensions handled by the endpoint you are provisioning. All endpoints sharing a prefix must use this addendum - in other words, you cannot have endpoint 1 with just prefix 1, and endpoint 2 with prefix 1 plus a range of extensions.

After provisioning each endpoint and before leaving the endpoint configuration mode you must enable the endpoint.

If you try to provision an endpoint with a location ID that is already in use, and if both location ID and endpoint type actually match the existing one, you will re-configure the first one. If the location ID and the type do not match the existing one, the system will warn you, for example, “Invalid endpoint type.

The specified type does not match the existing endpoint." If you use a location ID similar to one already in your network, the system will warn you, for example, "Possible conflict with existing location ID(s): 3, 333."

To delete an endpoint, see "Deleting or Clearing Endpoints" on page 75.

**Note** The system does not allow you to change the configurations for an autoregistered endpoint.

## Prerequisites

In the following, note that what Cisco UMG refers to as **endpoint** *location-id* is the same as the Cisco Unity Express **network location-id** *number*.

For each endpoint type, you have different parameters to set:

***Table 8 Endpoint Types: Cisco Unity Express 3.0 or earlier versions***

| Keyword | Description |
|---|---|
| **broadcast-id** *broadcast-id* | (Optional) Endpoint's broadcast ID. This is an alphanumeric string (range: 1-32) that cannot include spaces. |
| **domain** *domain* | Fully qualified name of domain to which endpoint belongs; for example, sj.mycompany.com. |
| **messaging-gateway secondary** *location-id* | (Optional) Location ID of secondary messaging-gateway. |
| **hostname** *hostname* | Endpoint's hostname or IP address. |
| **prefix** *prefix* | Messaging system telephone number prefix—phone number prefix that is added to a subscriber's extension (range: 1-15 digits). |
| **extension** *extension* | Subscribers' extension (range: 1-15 digits). |

***Table 9 Endpoint Types: Cisco Unity***

| Keyword | Description |
|---|---|
| **domain** *domain* | Fully qualified name of domain to which endpoint belongs; for example, sj.mycompany.com |
| **hostname** *hostname* | Endpoint's hostname or IP address. |
| **messaging-gateway secondary** *location-id* | Location-ID of the endpoint's secondary messaging gateway. |
| **prefix** *prefix* | Messaging system telephone number prefix that is added to a subscriber's extension (range: 1-15 digits). |
| **extension** *extension* | Subscribers' extension (range: 1-15 digits). |
| **serial-number** *serial-number* | (Optional) Endpoint's serial number. |

*Table 10 Endpoint Types: Avaya Interchange*

| Keyword | Description |
|---|---|
| **domain** *domain* | Fully qualified name of endpoint's domain; for example, sj.mycompany.com.. |
| **hostname** *hostname* | Endpoint's hostname or IP address. |
| **prefix** *prefix* | Messaging system telephone number prefix—phone number prefix that is added to a subscriber's extension (maximum 15 digits) |
| **extension** *extension* | Subscribers' extension (range: 1-15 digits). |

**Note** Avaya Interchange does not support a secondary messaging gateway.

**Note** When you use a **show** command to display the domain name, only the truncated name appears; for example, "mycompany".

**Note** The **default** command available in the endpoint configuration mode serves as an alternative to the **no** command when used in combination with any of the other commands available in that mode; for example, **hostname default**.

## SUMMARY STEPS

1. **config t**
2. **endpoint** *location-id* **{ unity | interchange | cue }**
3. **hostname** *hostname*
4. (Optional) **messaging-gateway secondary** *location-id*
5. **domain** *domain*
6. Either:
   a. **prefix** *prefix*
      or
   b. **prefix** *prefix* **number-only**
      **extension** *extension*
      **end**
7. (Optional) **broadcast-id** *broadcast-id*
8. (Optional) **serial-number** *serial-number*
9. **enable**
10. **end**
11. **end**
12. **show endpoint** { **local | network** } [*location-id* | **filter** *filter* ]
13. **show mailbox** {*location-id* | **prefix** *prefix* } [ *mailbox* | **filter** *filter* ]

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **config t**<br><br>**Example:**<br>`umg-1# config t` | Enters configuration mode. |
| **Step 2** | **endpoint** *location-id* **{ unity \| interchange \| cue }**<br><br>**Example:**<br>`umg-1(config)# endpoint 77777 unity` | Enters endpoint configuration mode and identifies the endpoint to be provisioned by location and type. |
| **Step 3** | **hostname** *hostname*<br><br>**Example:**<br>`umg-1(config-endpoint)# unity-7` | Specifies the endpoint's hostname or IP address. |
| **Step 4** | **messaging-gateway secondary** *location-id*<br><br>**Example:**<br>`umg-1(config-endpoint)# messaging-gateway secondary 51000` | (Optional) Specifies the endpoint's secondary messaging gateway by means of its location ID.<br><br>**Note** Avaya Interchange does not support secondary messaging gateways. |
| **Step 5** | **domain** *domain*<br><br>**Example:**<br>`umg-1(config-endpoint)# domain sj.mycompany.com` | Specifies the endpoint's domain name. |
| **Step 6** | **a) prefix** *prefix*<br><br>**Example:**<br>`umg-1(config-endpoint)# prefix 231`<br><br>b) **prefix** *prefix* **number-only**<br>**extension** *extension*<br>**end**<br><br>**Example:**<br>`umg-1(config-endpoint)# prefix 231 number-only`<br>`umg-1(config-endpoint-extension)# extension 777`<br>`umg-1(config-endpoint-extension)# end` | **a.** Specifies the endpoint's phone number prefix (range: 1-9 digits).<br>**b.** Specifies the prefix, enters endpoint extension configuration mode, specifies the range of extensions (range:1-15 digits), and then leaves endpoint extension configuration mode.<br><br>**Note** If you have multiple endpoints with the same prefix, you must use the **number-only** addendum (keyword) to the **prefix** command to specify the range of extensions handled by the endpoint you are provisioning. |
| **Step 7** | **broadcast-id** *broadcast-id*<br><br>**Example:**<br>`umg-1(config-endpoint)# broadcast-id 222222` | (Optional) Specifies the endpoint's broadcast ID, an alphanumeric string (range: 1-10); cannot include spaces).<br><br>Avaya Interchange does not support the broadcast messaging function. |
| **Step 8** | **serial-number** *serial-number*<br><br>**Example:**<br>`umg-1(config-endpoint)# serial-number-13` | (Optional) Specifies the endpoint's serial number. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 9** | **enable**<br><br>**Example:**<br>`umg-1(config-endpoint)# enable` | Enables the endpoint. |
| **Step 10** | **end**<br><br>**Example:**<br>`umg-1(config-endpoint)# end` | Exits endpoint configuration mode and enters configuration mode. |
| **Step 11** | **end**<br><br>**Example:**<br>`umg-1(config-endpoint)# end` | Exits configuration mode. |
| **Step 12** | **show endpoint { local \| network }** [*location-id* \| **filter** *filter* ]<br><br>**Example:**<br>`umg-1# show endpoint local 77777` | Displays a list of local or remote endpoints on the current configuring messaging gateway.<br>If you have many endpoints, you might get this message:<br>"Too many results, please use filter to limit the search result. Only the first 500 endpoints will be displayed."<br>The filter is any part of a location ID. For example, if you had the location IDs 123, 234, and 345 and you used a filter of 23 you would match 123 and 234. If you used a filter of 34 you would match 234 and 345.<br>Regular expressions are not supported. |
| **Step 13** | **show mailbox** {*location-id* \| **prefix** *prefix* } [ *mailbox* \| **filter** *filter* ]<br><br>**Example:**<br>`umg-1# show mailbox 77777` | Displays a list of the mailboxes associated with the specified endpoint. |

## Examples

The following example is an example of how to manually provision a Cisco Unity endpoint. An endpoint of this type requires a prefix, and because the number-only attribute has been used, it can be safely assumed that at least two of the user's Cisco Unity endpoints are using the same prefix.

```
umg-1# config t
umg-1(config)# endpoint 77777 unity
umg-1(config-endpoint)# messaging-gateway secondary 51000
umg-1(config-endpoint)# domain sj.mycompany.com
umg-1(config-endpoint)# hostname unity-7
umg-1(config-endpoint)# prefix 231 number-only
umg-1(config-endpoint-extension)# extension 777
umg-1(config-endpoint-extension)# end
umg-1(config-endpoint)# serial-number 13
umg-1(config-endpoint)# broadcast-id 222222
umg-1(config-endpoint)# enable
umg-1(config-endpoint)# end
umg-1(config)# end
se-10-1-12-95# show endpoint local 77777
Location Id:           77777
Hostname:              unity-7
Domain:                sj.mycompany.com
Prefix:                231
NAT:                   Enabled
Type:                  Unity
Serial-number:         13
Addressing Mode:       Number-only
Primary Gateway ID:    50000
Secondary Gateway ID:  51000
Status:                Disabled
umg-1#
```

# Setting Up NAT Entries

If you have NAT devices in your network, and they are between messaging gateways and/or endpoints, you must configure NAT entries on Cisco UMG for both messaging gateways and endpoints. For a message to reach its destination, Cisco UMG must know the external HTTP IP address and port number and the external VPIM IP address and port number of the NAT device in front of the destination.

**Note** When multiple messaging gateways are behind the same NAT device, configure the endpoints so that they can talk to messaging gateways on ports other than 80/25, because multiple endpoints may be sharing the same external IP address.
(When Cisco Unity Express registers with Cisco UMG, it has the option to specify the HTTP and SMTP ports to match the external PORT used in your setup. For reference, see "Appendix A: Cisco Unity Express Endpoint Autoregistration to Cisco Unified Messaging Gateway 1.0" on page 91)

## Prerequisites

For each endpoint and peer messaging gateway in your system, the following information is required to set up NAT entries:

- Location ID of the device
- VPIM external IP address and listening port
- HTTP external IP address and listening port

### SUMMARY STEPS

1. **config t**
2. **nat location** *location-id*
3. **http external** *ip port*
4. **vpim external** *ip port*
5. **end**
6. **end**
7. **show nat location** *location-id*

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **config t**<br><br>**Example:**<br>umg-1# config t | Enters configuration mode. |
| **Step 2** | **nat location** *location-id*<br><br>**Example:**<br>umg-1(config)# nat location 77777 | Enters NAT configuration mode to configure NAT settings for the specified device. |
| **Step 3** | **http external** *ip port*<br><br>**Example:**<br>umg-1(config-nat)# http external 192.0.2.13 8080 | Configures NAT entry for HTTP protocol, setting external IP address and listening port (default port is 80). |
| **Step 4** | **vpim external** *ip port*<br><br>**Example:**<br>umg-1(config-nat)# vpim external 192.0.2.13 26 | Configures NAT entry for VPIM protocol, setting external IP address and listening port (default port is 25). |
| **Step 5** | end<br><br>**Example:**<br>umg-1(config-nat)# end | Exits NAT configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **end**<br><br>**Example:**<br>`umg-1(config)# end` | Exits configuration mode. |
| **Step 7** | **show nat location** *location-id*<br><br>**Example:**<br>`umg-1# show nat location 77777` | Lists out configured NAT entries for the device. |

## Examples

The following example illustrates the the method for configuring NAT.

```
umg-1# config t
umg-1(config)# nat location 77777
umg-1(config-nat)# vpim external 192.0.2.13 26
umg-1(config-nat)# http external 192.0.2.13 8080
umg-1(config-nat)# end
umg-1(config)# end
umg-1# show nat location 77777
Protocol    Ext-IP             Ext-Port
---------------------------------------
HTTP        192.0.2.13         8080
SMTP        192.0.2.13         26

umg-1#
```

# Configuring NTP Servers

During the software postinstallation process, the Network Time Protocol (NTP) server may have been configured. If it was not configured, or if you want to change the configuration, use this procedure to add or delete NTP servers. Cisco UMG supports up to three NTP servers.

## Adding NTP Servers

You can specify an NTP server using its IP address or its hostname.

Cisco UMG uses the DNS server to resolve the hostname to an IP address and stores the IP address as an NTP server. If DNS resolves the hostname to more than one IP address, Cisco UMG randomly chooses one of the IP addresses that is not already designated as an NTP server. If you do not want to go with random choice, set the **prefer** attribute for one server.

To configure an NTP server with multiple IP addresses for a hostname, repeat the configuration steps using the same hostname. Each iteration assigns the NTP server to its remaining IP addresses.

### SUMMARY STEPS

1. **config t**
2. **ntp server** {*hostname* | *ip-address*} [ **prefer** ]
3. **end**
4. **show ntp status**
5. **show ntp configuration**
6. **copy running-config startup-config**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **config t**<br><br>**Example:**<br>`umg-1# config t` | Enters configuration mode. |
| **Step 2** | **ntp server** {*hostname* \| *ip-address*} [ **prefer** ]<br><br>**Example:**<br>`umg-1(config)# ntp server 192.0.2.14`<br>`umg-1(config)# ntp server 192.0.2.17 prefer` | Specifies the hostname or IP address of the NTP server.<br><br>If more than one server is configured, the server with the **prefer** attribute is used before the others. |
| **Step 3** | **end**<br><br>**Example:**<br>`umg-1(config)# exit` | Exits configuration mode. |
| **Step 4** | **show ntp status**<br><br>**Example:**<br>`umg-1# show ntp status` | Displays the NTP subsystem status. |
| **Step 5** | **show ntp configuration**<br><br>**Example:**<br>`umg-1# show ntp configuration` | Displays the configured NTP servers. |
| **Step 6** | **copy running-config startup-config**<br><br>**Example:**<br>`umg-1# copy running-config startup-config` | Copies the configuration changes to the startup configuration. |

## Examples

The following commands configure the NTP server:

```
umg-1# config t
umg-1(config)# ntp server 192.0.2.14
umg-1(config)# exit
umg-1#
```

The output from the **show ntp status** command looks similar to the following:

```
umg-1# show ntp status

NTP reference server 1:       10.100.6.9
Status:                       sys.peer
Time difference (secs):       3.268110099434328E8
Time jitter (secs):           0.1719226837158203
umg-1#
```

The following example configures an NTP server with a hostname that points to two IP addresses, 192.0.2.14 and 192.0.2.13:

```
umg-1# config t
umg-1(config)# ntp server NTP.mine.com
umg-1(config)# exit
umg-1#

umg-1# config t
umg-1(config)# ntp server NTP.mine.com
umg-1(config)# exit
umg-1#
```

The output from the **show ntp status** command might look similar to the following:

```
umg-1# show ntp status

NTP reference server 1:       192.0.2.14
Status:                       sys.peer
Time difference (secs):       3.268110099434328E8
Time jitter (secs):           0.1719226837158203

NTP reference server 1:       192.0.2.13
Status:                       sys.peer
Time difference (secs):       3.268110099434328E8
Time jitter (secs):           0.1719226837158203
umg-1#
```

# Removing an NTP Server

Remove an NTP server using its IP address or hostname.

## SUMMARY STEPS

1. **config t**
2. **no ntp server** {*hostname* | *ip-address*}
3. **exit**
4. **show ntp status**
5. **show ntp configuration**
6. **copy running-config startup-config**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **config t**<br><br>**Example:**<br>`umg-1# config t` | Enters configuration mode. |
| **Step 2** | **no ntp server** {*hostname* \| *ip-address*}<br><br>**Example:**<br>`umg-1(config)# no ntp server 192.0.2.14`<br>`umg-1(config)# no ntp server myhost` | Specifies the hostname or IP address of the NTP server to remove. |
| **Step 3** | **exit**<br><br>**Example:**<br>`umg-1(config)# exit` | Exits configuration mode. |
| **Step 4** | **show ntp status**<br><br>**Example:**<br>`umg-1# show ntp status` | Displays the NTP subsystem status. |
| **Step 5** | **show ntp configuration**<br><br>**Example:**<br>`umg-1# show ntp configuration` | Displays the configured NTP servers. |
| **Step 6** | **copy running-config startup-config**<br><br>**Example:**<br>`umg-1# copy running-config startup-config` | Copies the configuration changes to the startup configuration. |

# Displaying NTP Server Information

The following commands are available to display NTP server configuration information and status:

- **show ntp associations**
- **show ntp servers**
- **show ntp source**
- **show ntp status**

The following is sample output for the **show ntp associations** command:

```
umg-1# show ntp associations

ind assID status  conf reach auth condition  last_event cnt
===========================================================
  1 61253  8000   yes   yes  none    reject
```

The following is sample output for the **show ntp servers** command:

```
umg-1# show ntp servers

     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 1.100.6.9       0.0.0.0         16 u    - 1024    0    0.000    0.000 4000.00
space reject,       x falsetick,       . excess,          - outlyer
+ candidate,        # selected,        * sys.peer,        o pps.peer
```

The following is sample output for the **show ntp source** command:

```
umg-1# show ntp source

127.0.0.1: stratum 16, offset 0.000013, synch distance 8.67201
0.0.0.0:        *Not Synchronized*
```

The following is sample output for the **show ntp status** command:

```
umg-1# show ntp status

NTP reference server :        10.100.6.9
Status:                       reject
Time difference (secs):       0.0
Time jitter (secs):           4.0
```

# Setting the Time Zone

Typically, you set the time zone during installation. If you did not, or you want to change it, to set the time zone, use the **clock timezone** command in Cisco UMG configuration mode. The system will offer you a range of options to choose from.

To display the time zone, use the **show clock** command in Cisco UMG EXEC mode.

## Examples

```
umg-1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
umg-1(config)# clock timezone
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa            4) Arctic Ocean     7) Australia       10) Pacific Ocean
2) Americas          5) Asia             8) Europe
3) Antarctica        6) Atlantic Ocean   9) Indian Ocean
#? 2
Please select a country.
 1) Anguilla              18) Ecuador              35) Paraguay
 2) Antigua & Barbuda     19) El Salvador          36) Peru
 3) Argentina             20) French Guiana        37) Puerto Rico
 4) Aruba                 21) Greenland            38) St Kitts & Nevis
 5) Bahamas               22) Grenada              39) St Lucia
 6) Barbados              23) Guadeloupe           40) St Pierre & Miquelon
 7) Belize                24) Guatemala            41) St Vincent
 8) Bolivia               25) Guyana               42) Suriname
 9) Brazil                26) Haiti                43) Trinidad & Tobago
10) Canada                27) Honduras             44) Turks & Caicos Is
11) Cayman Islands        28) Jamaica              45) United States
12) Chile                 29) Martinique           46) Uruguay
13) Colombia              30) Mexico               47) Venezuela
14) Costa Rica            31) Montserrat           48) Virgin Islands (UK)
```

```
15) Cuba                  32) Netherlands Antilles  49) Virgin Islands (US)
16) Dominica              33) Nicaragua
17) Dominican Republic    34) Panama
#? 45
Please select one of the following time zone regions.
 1) Eastern Time
 2) Eastern Time - Michigan - most locations
 3) Eastern Time - Kentucky - Louisville area
 4) Eastern Time - Kentucky - Wayne County
 5) Eastern Standard Time - Indiana - most locations
 6) Eastern Standard Time - Indiana - Crawford County
 7) Eastern Standard Time - Indiana - Starke County
 8) Eastern Standard Time - Indiana - Switzerland County
 9) Central Time
10) Central Time - Michigan - Wisconsin border
11) Central Time - North Dakota - Oliver County
12) Mountain Time
13) Mountain Time - south Idaho & east Oregon
14) Mountain Time - Navajo
15) Mountain Standard Time - Arizona
16) Pacific Time
17) Alaska Time
18) Alaska Time - Alaska panhandle
19) Alaska Time - Alaska panhandle neck
20) Alaska Time - west Alaska
21) Aleutian Islands
22) Hawaii
#? 16

The following information has been given:

        United States
        Pacific Time

Therefore TZ='America/Los_Angeles' will be used.
Is the above information OK?
1) Yes
2) No
#? 1

Local time is now:      Mon Aug 27 17:23:54 PDT 2007.
Universal Time is now:  Tue Aug 28 00:23:54 UTC 2007.
Save the change to startup configuration and reload the module for the new timez
one to take effect.
umg-1(config)#
```

# Configuring Logging Operations

Cisco UMG captures messages that describe activities in the system. These messages are collected and directed to a messages.log file on the Cisco UMG module hard disk, the console, or an external system log (syslog) server. The messages.log file is the default destination.

This section describes the procedure for configuring an external server to collect the messages. To view the messages, see "Viewing System Activity Messages" on page 57.

**Note** The external server must be configured to listen on UDP port 514 for traffic coming from the IP address of the Cisco UMG.

## Prerequisites

You need the hostname or IP address of the designated log server.

### SUMMARY STEPS

1. **config t**
2. **log server address** {*hostname* | *ip-address*}
3. **exit**
4. **show running-config**

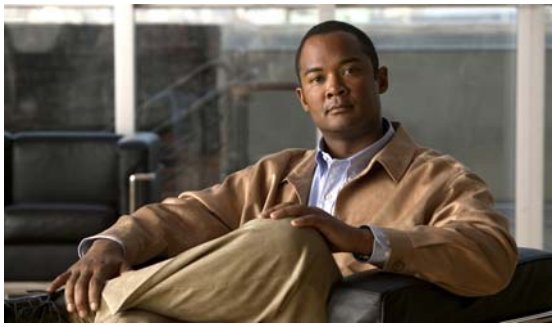
### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **config t**<br><br>**Example:**<br>umg-1# config t | Enters configuration mode. |
| **Step 2** | **log server address** {*hostname* \| *ip-address*}<br><br>**Example:**<br>umg-1(config)# **log server address 10.187.240.31**<br>umg-1(config)# **log server address logpc** | Specifies the hostname or IP address of the NTP server designated as the log server. |
| **Step 3** | **exit**<br><br>**Example:**<br>umg-1(config)# exit | Exits configuration mode. |
| **Step 4** | **show running-config**<br><br>**Example:**<br>umg-1# show running-config | Displays the system configuration, which includes the configured log server. |

## Examples

The output from the **show running-config** command looks similar to the following:

```
umg-1# show running-config

clock timezone America/Los_Angeles
hostname umg-1
ip domain-name localdomain
ntp server 192.0.2.13
log server address 192.0.2.14
```



# Backing Up and Restoring Data

**Last updated: April 13, 2010**

Cisco Unified Messaging Gateway backup and restore functions use an FTP server to store and retrieve data. The backup function copies the files from the Cisco UMG module to the FTP server and the restore function copies the files from the FTP server to the Cisco UMG application. The FTP server can reside anywhere in the network as long as the backup and restore functions can access it with an IP address or hostname.

**Note** Setting up a backup server is part of the initial configuration process. If you have not already done this, see "Setting Backup Parameters" on page 22.

Do backups regularly to preserve configuration data.

Backing up and restoring both require offline mode, so they are best done when call traffic is least impacted. Before you take the system offline, decide what type of files you will back up:

- **all** files (configuration and data)
- **only data** files (includes dynamic data such as local endpoint IDs, mailboxes and system distribution lists)

**Caution** We strongly discourage doing the 'data only' type of backup and restore because of its potential to introduce inconsistency between configuration and data files.

- **only configuration** files (includes the local messaging gateway ID, messaging gateway peers, manually configured endpoints, registration credentials, and NAT data)

**Caution** Offline mode terminates message forwarding and directory exchange. We recommend doing backups when call traffic is least impacted.

This chapter contains the following sections:

# Restrictions

Cisco UMG does not support the following backup and restore capabilities:

- Scheduled backup and restore operations. The backup and restore procedures begin when the appropriate command is entered.
- Centralized message storage arrangement. Cisco UMG backup files cannot be used or integrated with other message stores.
- Selective backup and restore. Only full backup and restore functions are available. Individual messages or other specific data can be neither stored nor retrieved.

**Caution** If you delete an endpoint, then do a system restore, the update will erase the information that the endpoint was deleted. You must reset it from the endpoint's primary messaging gateway.

# Backing Up Files

Three types of backups are available: data only, configuration only, or all.

- Data—includes local endpoint IDs, mailboxes and system distribution lists (SDLs).
- Configuration—includes local peers, manually configured endpoints, credentials, and NAT.
- All—Backs up all data and configuration information.

Perform backups only in offline mode.

Cisco UMG automatically assigns a backup ID to each backup. Although there are the three different types of backups, backup ID assignment takes no account of data type, so that you would never find two backups with the same backup ID, even if one is a configuration file and the other a data file.

To determine the backup ID of the file you want to restore, use the **show backup server** or **show backup history** command in either EXEC or offline mode. That command lists all available back copies on the remote backup server and their respective backup IDs.

**Note** We recommend that you back up your configuration files whenever you make changes to the system or application files.

**Caution** Offline mode terminates all message forwarding. We recommend doing backups when call traffic is least impacted.

### SUMMARY STEPS

1. **offline**
2. **backup category** {**all** | **configuration** | **data**}
3. **continue**
4. **show backup history**
5. **show backup server**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **offline**<br><br>**Example:**<br>`umg-1# offline` | Enters offline mode. All message forwarding is terminated. |
| **Step 2** | **backup category** {**all** \| **configuration** \| **data**}<br><br>**Example:**<br>`umg-1(offline)# backup category all`<br>`umg-1(offline)# backup category configuration`<br>`umg-1(offline)# backup category data` | Specifies the type of data to be backed up and stored. |
| **Step 3** | **continue**<br><br>**Example:**<br>`umg-1(offline)# continue` | Exits offline mode and enters EXEC mode. |
| **Step 4** | **show backup history**<br><br>**Example:**<br>`umg-1# show backup history` | Displays the success or failure of the backup and restore procedures, and also the backup IDs. |
| **Step 5** | **show backup server**<br><br>**Example:**<br>`umg-1# show backup server` | Displays the backup files available on the backup server, the date of each backup, and the backup file ID. |

# Examples

The following examples display the output from the **show backup history** and **show backup server** commands:

```
umg-1# show backup history

#Start Operation
Category:      Configuration
Backup Server: ftp://10.100.10.215/umg-1_backup
Operation:     Backup
Backupid:      2
Restoreid:     -1
Description:   test backup 1
Date:          Sun Jun 13 12:32:48 PDT 1993
Result:        Success
Reason:
#End Operation

#Start Operation
Category:      Data
Backup Server: ftp://10.100.10.215/umg-1_backup
Operation:     Backup
Backupid:      2
Restoreid:     -1
Description:   umg-1 test backup
```

```
Date:          Sun Jun 13 12:32:57 PDT 1993
Result:        Success
Reason:
#End Operation

#Start Operation
Category:      Configuration
Backup Server: ftp://10.100.10.215/umg-1_backup
Operation:     Restore
Backupid:      2
Restoreid:     1
Description:
Date:          Sun Jun 13 12:37:52 PDT 1993
Result:        Success
Reason:
#End Operation

#Start Operation
Category:      Data
Backup Server: ftp://10.100.10.215/umg-1_backup
Operation:     Restore
Backupid:      2
Restoreid:     1
Description:
Date:          Sun Jun 13 12:38:00 PDT 1993
Result:        Success
Reason:
#End Operation


umg-1# show backup server

Category:       Data
Details of last 5 backups
Backupid:     1
Date:         Tue Jul 22 10:55:52 PDT 2003
Description:

Backupid:     2
Date:         Tue Jul 29 18:06:33 PDT 2003
Description:

Backupid:     3
Date:         Tue Jul 29 19:10:32 PDT 2003
Description:

Category:       Configuration
Details of last 5 backups
Backupid:     1
Date:         Tue Jul 22 10:55:48 PDT 2003
Description:

Backupid:     2
Date:         Tue Jul 29 18:06:27 PDT 2003
Description:


Backupid:     3
Date:         Tue Jul 29 19:10:29 PDT 2003
Description:

umg-1#
```

# Restoring Files

After you create the backup files, you can restore them when needed. Restoring is done in offline mode, which terminates all message forwarding calls. You should therefore consider restoring files when call traffic is least impacted.

To determine the backup ID of the file you want to restore, use the **show backup server** or **show backup history** command in either EXEC or offline mode.

## SUMMARY STEPS

1. **show backup server**
2. **offline**
3. **restore id** *backup-id* **category** {**all** | **configuration** | **data**}
4. **show backup history**
5. **reload**

## DETAILED STEPS

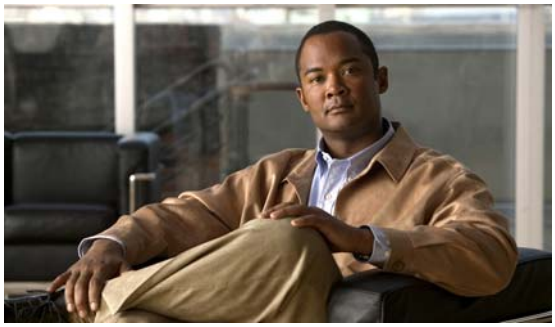
| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **show backup server**<br><br>**Example:**<br>`umg-1# show backup server` | Lists the data and configuration backup files. Look in the backup ID field for the revision number of the file that you want to restore. |
| **Step 2** | **offline**<br><br>**Example:**<br>`umg-1# offline` | Enters offline mode. All message forwarding is terminated. |
| **Step 3** | **restore id** *backupid* **category** {**all** \| **configuration** \| **data**}<br><br>**Example:**<br>`umg-1(offline)# restore id 22 category all`<br>`umg-1(offline)# restore id 8 category configuration`<br>`umg-1(offline)# restore id 3 category data` | Specifies the backup ID *backupid* value and the file type to be restored. |
| **Step 4** | **show backup history**<br><br>**Example:**<br>`umg-1# show backup history` | Displays the success or failure of backup and restore procedures, and also the backup IDs. |
| **Step 5** | **reload**<br><br>**Example:**<br>`umg-1(offline)# reload` | Resets Cisco UMG so that the restored values take effect. |

## Examples

The following examples display the contents of the backup server and the backup history:

```
umg-1# show backup server

Category:       Data
Details of last 5 backups
Backupid:     1
Date:         Tue Jul 22 10:55:52 PDT 2003
Description:

Backupid:     2
Date:         Tue Jul 29 18:06:33 PDT 2003
Description:

Backupid:     3
Date:         Tue Jul 29 19:10:32 PDT 2003
Description:

Category:       Configuration
Details of last 5 backups
Backupid:     1
Date:         Tue Jul 22 10:55:48 PDT 2003
Description:

Backupid:     2
Date:         Tue Jul 29 18:06:27 PDT 2003
Description:

Backupid:     3
Date:         Tue Jul 29 19:10:29 PDT 2003
Description:

umg-1#

umg-1# show backup history

Start Operation
Category:      Configuration
Backup Server: ftp://10.100.10.215/umg-1_backup
Operation:     Backup
Backupid:      1
Restoreid:     -1
Description:   test backup 1
Date:          Sun Jun 13 12:23:38 PDT 1993
Result:        Failure
Reason:        Script execution failed: /bin/BR_VMConfg_backup.sh: returnvalue:1
 ; Server Url:ftp://10.100.10.215/umg-1_backup: returnvalue:9 Unable to authenticate
#End Operation

#Start Operation
Category:      Data
Backup Server: ftp://10.100.10.215/umg-1_backup
Operation:     Backup
Backupid:      1
Restoreid:     -1
Description:   test backup 1
Date:          Sun Jun 13 12:23:44 PDT 1993
Result:        Failure
Reason:        Script execution failed: /bin/BR_VMData_backup.sh: returnvalue:1
Messaging Backup failed; Server Url:ftp://10.100.10.215/umg-1_backup: returnvalue:9
 Unable to authenticate
```

```
#End Operation

#Start Operation
Category:      Configuration
Backup Server: ftp://10.100.10.215/umg-1_backup
Operation:     Backup
Backupid:      2
Restoreid:     -1
Description:   umg-1 test backup
Date:          Sun Jun 13 12:32:48 PDT 1993
Result:        Success
Reason:
#End Operation

#Start Operation
Category:      Data
Backup Server: ftp://10.100.10.215/umg-1_backup
Operation:     Backup
Backupid:      2
Restoreid:     -1
Description:   umg-1 test backup
Date:          Sun Jun 13 12:32:57 PDT 1993
Result:        Success
Reason:
#End Operation
```



# Monitoring the Cisco Unified Messaging Gateway System

**Last updated: April 13, 2010**

This chapter contains procedures for monitoring the Cisco Unified Messaging Gateway system's health and performance and includes the following sections:



## Viewing Network Status

Use these commands to verify the status of peer messaging gateways and endpoints.

*Table 11 Network Status Commands*

| Command | Function |
|---|---|
| **show ddr timeout** | Displays lapse of time (in hours) after which the system generates a DDR for a message. Default is one hour. |
| **show endpoint local** | Displays a list of all the endpoints associated with the current Cisco UMG. |
| **show endpoint network** | Displays a list of all the endpoints associated with peer Cisco UMGs. |
| **show ndr timeout** | Displays lapse of time (in hours) after which the system generates an NDR for a message. Default is six hours. |
| **show registration block** | Displays a list of endpoints that are prevented from registering. |
| **show registration status** | Displays a list of registered endpoints and their status: whether online or not, and so on. |

*Table 11 Network Status Commands (continued)*

| Command | Function |
|---|---|
| **show registration users** | Displays the user credentials of the autoregistered endpoints. |
| **show spoken-name** | Indicates whether spoken-name has been enabled on the current configuring messaging gateway. |
| **show statistics** | Displays statistics relative to endpoints. |

# Locating and Viewing Individual Mailbox Details

To locate an individual mailbox in your system and view its details (the phone number, extension, and first and last names associated with the mailbox), use the following procedure.

This procedure assumes that you know the subscriber number, and that you do not know whether it is associated with a local or remote endpoint. It also assumes that you use the **show mailbox** command for each of the listed endpoints.

If you have provisioned your endpoints with prefixes, you can more easily identify which of the endpoints is worth searching. However, to find a mailbox, it is not sufficient to know the prefix associated with the mailbox's endpoint (unless each of your prefixes applies only to a single endpoint), you must know which endpoint the mailbox is associated with.

**Note** The system only displays the first 300 search results. If necessary, the system asks you to use a filter to limit the search results.

## SUMMARY STEPS

1. **show endpoint local**
2. **show mailbox** *location-id* **filter** *filter*
3. **show endpoint network** *location-id*
4. **show mailbox** *location-id* **filter** *filter*
5. **show mailbox** *location-id mailbox*

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **show endpoint local**<br><br>**Example:**<br>`umg-1# show endpoint local` | Displays all the endpoints associated with the current Cisco UMG, their location IDs, location prefixes, types, primary messaging gateways, and if applicable, secondary messaging gateways. |
| **Step 2** | **show mailbox** *location-id* **filter** *filter*<br><br>**Example:**<br>`umg-1# show mailbox 300 filter 0100` | Displays all the mailboxes associated with the specified endpoint, filtered by subscriber extension. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **Example:**<br>**show endpoint network** *location-id*<br><br>**Example:**<br>umg-1# **show endpoint network** | Displays all the endpoints associated with peer messaging gateways, their location IDs, their location prefixes, their types, their primary messaging gateways, and if applicable, their secondary messaging gateways. |
| **Step 4** | **show mailbox** *location-id* **filter** *filter*<br><br>**Example:**<br>umg-1# show mailbox 7 filter 0100 | Displays all the mailboxes associated with the specified endpoint, filtered by subscriber extension. |
| **Step 5** | **show mailbox** *location-id* *mailbox*<br><br>**Example:**<br>umg-1# show mailbox 7 4085550100 | Displays the details of the specified mailbox, that is, extension, first name and last name of the subscriber. |

## Examples

The following example illustrates the output for the **show endpoint local**, **show endpoint network**, and **show mailbox** commands when used in the sequence described previously:

```
se-10-1-12-96# show endpoint local
A total of 8 local endpoint(s) have been found:

Location    Location          Endpoint     Endpoint  Primary     Secondary
ID          Prefix            Type         Status    Gateway     Gateway
-------------------------------------------------------------------------
300         408555            CUE          Offline   51000
365         408555            CUE          Offline   51000
366         408555            CUE          Offline   51000
369         408555            CUE          Offline   51000
370         408555            CUE          Offline   51000
375         408109            CUE          Offline   51000
376         408110            CUE          Offline   51000
379         408111            CUE          Offline   51000

umg-1# show mailbox prefix 408555 filter 0100
No mailbox has been found for prefix 408555(filter='0100').
umg-1# show endpoint network
A total of 259 network endpoint(s) have been found:

Location    Location          Endpoint     Primary     Secondary
ID          Prefix            Type         Gateway     Gateway
-------------------------------------------------------------
1           408101            CUE          50000
2           408102            CUE          50000
3           408103            CUE          50000
4           408104            CUE          50000
5           408105            CUE          50000
6           408555            CUE          50000
7           408555            CUE          50000
8           408108            CUE          50000
[...]
umg-1# show mailbox prefix 408555 filter 0100
1 mailbox(s) has been found for prefix 408555(filter='0100).
umg-1# show mailbox 7 4085550100
Phone:      4085550100
Extension:  0100
```

```
First Name: John
Last Name:  Doe
```

# Displaying Management Data Activity

Use the following commands in Cisco UMG EXEC mode to display management data activity:

- **trace management agent { all | debug }** —Enables tracing of management data requests.
- **trace management all**
- show trace buffer tail

The following example displays sample output of the **show trace buffer tail** command:

```
umg-1# show trace buffer tail 10
Press <CTRL-C> to exit...
2037 10/30 02:57:35.484 umg dirx 0 com.cisco.umg.direx.thread.MessageProcessorSc
heduler:Processor schdler woke up
2037 10/30 02:57:35.491 umg dirx 0 com.cisco.umg.direx.thread.MessageProcessorSc
heduler:Processor schdler going back to sleep
2037 10/30 03:02:35.492 umg dirx 0 com.cisco.umg.direx.thread.MessageProcessorSc
heduler:Processor schdler woke up
2037 10/30 03:02:35.495 umg dirx 0 com.cisco.umg.direx.thread.MessageProcessorSc
heduler:Processor schdler going back to sleep
2037 10/30 03:07:35.500 umg dirx 0 com.cisco.umg.direx.thread.MessageProcessorSc
heduler:Processor schdler woke up
2037 10/30 03:07:35.503 umg dirx 0 com.cisco.umg.direx.thread.MessageProcessorSc
heduler:Processor schdler going back to sleep
2037 10/30 03:12:35.504 umg dirx 0 com.cisco.umg.direx.thread.MessageProcessorSc
heduler:Processor schdler woke up
2037 10/30 03:12:35.507 umg dirx 0 com.cisco.umg.direx.thread.MessageProcessorSc
heduler:Processor schdler going back to sleep
2037 10/30 03:17:35.508 umg dirx 0 com.cisco.umg.direx.thread.MessageProcessorSc
heduler:Processor schdler woke up
2037 10/30 03:17:35.511 umg dirx 0 com.cisco.umg.direx.thread.MessageProcessorSc
heduler:Processor schdler going back to sleep
```

# Checking Hard Disk Memory Wear Activity

Cisco UMG tracks the use and wear of the hard disk memory as log and trace data are saved to the module. To display this data, use the **show interface ide 0** command in Cisco UMG EXEC mode.

**show interface ide 0**

## Examples

The following is sample output:

```
umg-1# show interface ide 0

IDE hd0 is up, line protocol is up
     218224 reads, 1941088256 bytes
     0 read errors
     2208286 write, 27276906496 bytes
     0 write errors
```

# Viewing System Activity Messages

Cisco UMG captures messages that describe activities in the system. The messages are categorized according to the impact on the system of the activity described in the message:

- Information—Describes normal system activity.
- 3_debug--Describes debugging activity
- 2_warn—An alert that a non-normal activity is occurring. The Cisco UMG system continues to function.
- 1_error—Indicates that a system error has occurred. The Cisco UMG system may have stopped functioning.
- 0_crash—Describes a critical situation with the system. The Cisco UMG system has stopped functioning.

These messages are collected and directed to three possible destinations:

- messages.log file—This option is the default. The file contains all system messages and resides on the Cisco UMG hard disk. You can view them on the console or copy them to a server to review for troubleshooting and error reporting.
- Console—View the system messages as they occur by using the **log console** command.
- External system log (syslog) server—Cisco UMG copies the messages to another server and collects them in a file on that server's hard disk. The syslog daemon configuration on the external server determines the directory to which the messages log will be saved.

**Note** To configure a syslog server, see "Configuring Logging Operations" on page 43. The external server must be configured to listen on UDP port 514 for traffic coming from your messaging gateway's IP address.

To view system activity, use the **log console monitor**, **log trace boot**, and **log trace buffer save** commands.

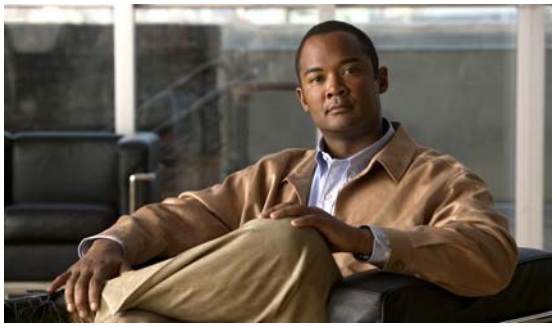
# Checking Log and Trace Files

To check the log and trace files on the hard disk, use the show logs command in Cisco UMG EXEC mode.

**show logs**

Logging and tracing to the hard disk is turned off by default. Executing the **log trace** command starts the log and trace functions immediately.

The command displays the **atrace.log** and **messages.log** files. Each file has a fixed length of 10 MB, and tracing or logging stops automatically when the file reaches this length. New files overwrite the old files.



# Maintaining the Cisco Unified Messaging Gateway System

**Last updated: April 13, 2010**

This chapter includes instructions for:



To back up Cisco UMG, see "Backing Up Files" on page 46.

To restore backup files - see "Restoring Files" on page 49.

For troubleshooting, see "Troubleshooting" on page 79.

## Copying Configurations

The following Cisco UMG EXEC commands are available to copy the startup configuration and running configuration to and from the hard disk on the Cisco UMG module, the network FTP server, and the network TFTP server.

**Note** Depending on the specific TFTP server you are using, you might need to create a file with the same name on the TFTP server and verify that the file has the correct permissions before transferring the running configuration to the TFTP server.

# Copying the Startup Configuration from the Hard Disk to Another Location

Starting in Cisco UMG EXEC mode, use the following command to copy the startup configuration on the hard disk to another location:

**copy startup-config** {**ftp:** *user-id*:*password*@*ftp-server-url* | **tftp:***tftp-server-url*}

**Syntax Description**

| | |
|---|---|
| **ftp:** *user-id*:*password*@ | Username and password for the FTP server. Include the colon (:) and the at sign (@) in your entry. |
| ftp-server-url | URL of the FTP server including directory and filename (e.g. ftps://server/dir/filename) |
| **tftp:***tftp-server-url* | URL of the TFTP server including directory and filename (e.g. tftps://server/dir/filename) |

This command is interactive and prompts you for the information. You cannot enter the parameters in one line. The following examples illustrate this process.

In this example, the startup configuration is copied to the FTP server, which requires a username and password to transfer files. The startup configuration file is saved on the FTP server with the filename **start**.

```
umg-1# copy startup-config ftp
Address or name of remote host? admin:messaging@ftps://server/dir/start
Source filename? temp_start
```

The following example shows the startup configuration copied to the TFTP server, which does not require a username and password. The startup configuration is saved in the TFTP directory **configs** as filename **temp_start**.

```
umg-1# copy startup-config tftp
Address or name of remote host? tftps://server/dir/temp_start
Source filename? temp_start
```

**Note** Depending on the specific TFTP server you are using, you might need to create a file with the same name on the TFTP server and verify that the file has the correct permissions before transferring the running configuration to the TFTP server.

# Copying the Startup Configuration from the Network FTP Server to Another Location

Starting in Cisco UMG EXEC mode, use the following command to copy the startup configuration on the network FTP server to another location:

**copy ftp: {running-config | startup-config}** ***user-id:password*@ftps://*server/dir/filename**

**Syntax Description**

| | |
|---|---|
| **running-config** | Active configuration on hard disk. |
| **startup-config** | Startup configuration on hard disk. |
| *user-id***:***password*@ | Username and password for the FTP server. Include the colon (:) and the at sign (@) in your entry. |
| *ftp-server-url* | URL of the FTP server. |

This command is interactive and prompts you for the information. You cannot enter the parameters in one line. The following example illustrates this process.

## Examples

In this example, the FTP server requires a username and password. The file start in the FTP server configs directory is copied to the startup configuration.

```
umg-1# copy ftp: startup-config
!!!WARNING!!! This operation will overwrite your startup configuration.
Do you wish to continue[y]? y
Address or name or remote host? admin:messaging@tftps://server/configs
Source filename? start
```

**Note** Depending on the specific TFTP server you are using, you might need to create a file with the same name on the TFTP server and verify that the file has the correct permissions before transferring the running configuration to the TFTP server.

# Copying the Running Configuration from the Hard Disk to Another Location

Starting in Cisco UMG EXEC mode, use the following command to copy the running configuration on the hard disk to another location:

**copy running-config {ftp:** *user-id:password*@**ftps://***server/dir/filename* **|**
**startup-config | tftp:tftps://***server/dir/filename* **}**

**Syntax Description**

| | |
|---|---|
| **ftp:** *user-id***:***password*@ | Username and password for the FTP server. Include the colon (:) and the at sign (@) in your entry. |
| *ftp-server-url* | URL of the FTP server including directory and filename.. |
| **startup-config** | Startup configuration on hard disk. |
| **tftp-server-url** | URL of the TFTP server including directory and filename. |

When you copy the running configuration to the startup configuration, enter the command on one line.

When you copy to the FTP or TFTP server, this command becomes interactive and prompts you for the information. You cannot enter the parameters in one line. The following example illustrates this process.

## Examples

In the following example, the running configuration is copied to the FTP server, which requires a username and password. The running configuration is copied to the configs directory as file saved_start.

```
umg-1# copy running-config ftp:
Address or name of remote host? admin:messaging@ftps://server/configs
Source filename? saved_start
```

In the following example, the running configuration is copied to the startup configuration. In this instance, enter the command on a single line.

```
umg-1# copy running-config startup-config
```

**Note** Depending on the specific TFTP server you are using, you might need to create a file with the same name on the TFTP server and verify that the file has the correct permissions before transferring the running configuration to the TFTP server.

# Copying the Running Configuration from the Network TFTP Server to Another Location

Starting in Cisco UMG EXEC mode, use the following command to copy the running configuration from the network TFTP server to another location:

**copy tftp:** {**running-config** | **startup-config**} **tftps:**//*server/dir/filename*

**Syntax Description**

| | |
|---|---|
| **running-config** | Active configuration on hard disk. |
| **startup-config** | Startup configuration on harddisk. |
| *tftp-server-url* | URL of the TFTP server. |

This command is interactive and prompts you for the information. You cannot enter the parameters in one line. The following example illustrates this process.

## Examples

In this example, the file start in directory **configs** on the TFTP server is copied to the startup configuration.

```
umg-1# copy tftp: startup-config
!!!WARNING!!! This operation will overwrite your startup configuration.
Do you wish to continue[y]? y
Address or name of remote host? tftps://server/configs
Source filename? start
```

**Note** Depending on the specific TFTP server you are using, you might need to create a file with the same name on the TFTP server and verify that the file has the correct permissions before transferring the running configuration to the TFTP server.

# Restoring Factory Default Values

Cisco UMG provides a command to restore the factory default values for the entire system. Restoring the system to the factory defaults erases the current configuration. This function is available in offline mode. When the system is clean, you see a message that the system will reload, and the system begins to reload. When the reload is complete, the system prompts you to go through the postinstallation process.

**Caution** This operation is irreversible. All data and configuration files are erased. Use this feature with caution. We recommend that you do a full system backup before proceeding with this feature.

Perform the following steps to reset the system to Cisco UMG factory default values.

**Step 1** `umg-1#` **offline**

This command puts the system into offline mode.

**Step 2** `umg-1(offline)#` **restore factory default**

```
This operation will cause all the configuration and data on the system to be erased. This
operation is not reversible. Do you wish to continue? (n)
```

**Step 3** Do one of the following:

- Enter **n** if want to retain the system configuration and data.

  The operation is cancelled, but the system remains in offline mode. To return to online mode, enter **continue**.

- Enter **y** if you want to erase the system configuration and data.

  When the system is clean, a message appears indicating that the system will start to reload. When the reload is complete, a prompt appears to start the postinstallation process.

# Going Offline, Reloading, Rebooting, Shutting Down, and Going Back Online

You must take the Cisco UMG system offline before you can do any backups, reload, or restore. However, you do not go offline before shutting down the system.

Always shut down Cisco UMG before power-cycling the router to avoid data loss or file corruption.

## Going Offline

Using the **offline** command in Cisco UMG EXEC mode takes the system into offline/administration mode and terminates all directory exchanges and message forwarding. All outstanding messages will be stored for processing when the system goes back online. When you use the **offline** command, the system asks for confirmation. The default is **no**, so to confirm, you must enter **yes**.

**Step 1** **offline**

**Step 2** **y**

## Examples

```
umg-1# offline
!!!WARNING!!!: If you are going
offline to do a backup, it is
recommended
that you save the current
running configuration using the
'write' command,
prior to going to the offline
state.
Putting the system offline will
terminate all end user sessions.
Are you sure you want to go
offline[n]? :y
umg-1(offline)
```

# Restarting Cisco UMG

To restart the system using the starting configuration, use the **reload** and **boot disk** commands in Cisco UMG offline/administration mode. Restarting the system will terminate all end-user sessions and cause any unsaved configuration data to be lost.

**Step 1** **reload**

**Step 2** **boot disk**

## Examples

```
umg-1(offline) reload
umg-1(offline)>
MONITOR SHUTDOWN...
EXITED: probe exit status 0
EXITED: SQL_startup.sh exit status 0
EXITED: LDAP_startup.sh exit status 0
[...]
Booting from Secure secondary boot loader..., please wait.

[BOOT-ASM]


Please enter '***' to change boot configuration:


 ServicesEngine Bootloader Version : eng_bld


ServicesEngine boot-loader boot disk
[...]
STARTED: /bin/products/umg/umg_startup.sh

 waiting 70 ...
SYSTEM ONLINE
umg-1#
```

# Shutting Down

To halt the system, use the **shutdown** command in Cisco UMG EXEC mode. Shutting down Cisco UMG not only terminates all directory exchange and message forwarding and causes any unsaved configuration data to be lost; it also causes all registered endpoints to go offline.

These instructions apply to shutting down the software. The procedure for the hardware is described in the "Hardware" section on page 65.

The procedure for online insertion and removal of the Cisco UMG network module is described in the hardware installation guide, at http://www.cisco.com/en/US/docs/routers/access/3800/hardware/installation/guide/hw.html.

**Caution** You must shut down the software before you shut down the hardware.

### Software

**Step 1** **shutdown**

## Examples

```
umg-1# shutdown
```

### Hardware

Press the reset button on the network module faceplate for less than 2 seconds to perform a graceful shutdown of the hard disk before removing power from the router or before starting an online insertion and removal (OIR) sequence on the router. The application may take up to 2 minutes to fully shut down.

**Warning** **If you press the shutdown button for *more than 4 seconds*, an immediate, non-graceful shutdown of the hard disk will occur and may cause file corruption on the network module's hard disk. After a non-graceful shutdown, the HD and SYS LEDs remain lit. Press the shutdown button for *less than 2 seconds* to gracefully reboot the network module.**

# Going Back Online

The **continue** command takes the messaging gateway back online again. All endpoints previously marked 'offline' will be marked 'online' again.

**Step 1** **continue**

## Examples

```
umg-1(offline) continue
umg-1#
```

# Forcing Data Convergence

Data convergence normally takes place automatically, any time an endpoint (including the mailboxes associated with it) or a messaging gateway is added, deleted, or modified. You can also force directory exchange.

**Note** This operation applies only to Cisco Unity Express 3.1 and later versions.

Cisco UMG can request that one or all endpoints send their full directories, or just updates. The current configuring messaging gateway can request one or all peer messaging gateways to send their full directories or just updates.

The current configuring messaging gateway can also send either its full directory or just an update to all endpoints and messaging gateways in the system or to specified ones.

The following procedure requests a directory from an endpoint, then sends the current configuring Cisco UMG's updated directory to a peer messaging gateway.

## Prerequisites

The location IDs of the endpoints and/or messaging gateways with which directories or updates are to be exchanged.

### SUMMARY STEPS

1. **directory exchange endpoint request full** [ *location-id* ]
2. **directory exchange messaging-gateway send update**
3. **directory exchange messaging-gateway request update**
4. **show messaging-gateway**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **directory exchange endpoint request** { **full** [ *location-id* ] \| **update** [ *location-id* ] }<br><br>**Example:**<br>umg-1# directory exchange endpoint request full 42 | Requests an endpoint to send either its full directory or the update information.<br>**Note** This operation only applies to Cisco Unity Express 3.1 and later versions. |
| **Step 2** | **directory exchange messaging-gateway send { full [** *location-id* **] \| update [** *location-id* **] }**<br><br>**Example:**<br>umg-1# directory exchange messaging-gateway send update | Sends the current configuring messaging gateway's full directory or the update information |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **directory exchange messaging-gateway request** { **full** [ *location-id* ] \| **update** [ *location-id* ] }<br><br>**Example:**<br>umg-1# directory exchange messaging-gateway request update | Requests directory exchange updates from all peer messaging gateways. |
| **Step 4** | **show messaging-gateway** [*location-id*]<br><br>**Example:**<br>umg-1# show messaging-gateway | Displays the location ID and hostname of any peer messaging gateways that have been configured, whether NAT is enabled for any of them, and the location ID of the current configuring messaging gateway. If a location ID other than the current configuring messaging gateway is specified, displays the named details for the specified messaging gateway. |

## Examples

The following example illustrates requesting a full directory exchange from an endpoint, then sending out the current configuring Cisco UMG's directory update to all peer messaging gateways, and finally checking to make sure all peers were actually online to receive the update.

```
umg-1# directory exchange endpoint request full 42
umg-1# directory exchange messaging-gateway send update
umg-1# show messaging-gateway
LocationID     Hostname                                NAT
-------------------------------------------------------------
59000          209.165.200.224                         disabled
777776         peer-1.mycompany.com                    enabled

Local Gateway ID: 51000

umg-1#
```

# Managing System Distribution Lists

Cisco UMG enables subscribers to send messages to system distribution lists (SDLs) with recipients (list members) on remote endpoints.

To create an SDL, from EXEC mode, enter the list manager mode to lock list management on all peer Cisco UMGs. The purpose of locking is to prevent messaging gateways getting out of sync. When you have finished configuring SDLs, you must publish them to peer messaging gateways. You can publish to all messaging gateways or you can publish to individual messaging gateways.

If you leave list manager mode without publishing SDLs, the system will automatically publish to all peer messaging gateways.

If the system encounters an SDL lock on a peer messaging gateway, it will fail to lock, and will automatically exit list manager mode. In this situation, you can wait till the lock on the peer messaging gateway is released and/or exit by using the **exit** command.

It is possible that messaging gateways' SDLs can get out of sync. If this is the case, you will be warned when you attempt to lock SDLs. The system will tell you that the current configuring Cisco UMG is out of sync with other messaging gateways. In this case, determine which messaging gateway has the latest

SDL information (by using the **show list tracking version** command to look at the SDL version numbers), and publish from there. This will bring the other messaging gateway back into sync with the rest.

When you create an SDL, you must ensure the number you assign to it (which is also the number the authorized sender dials to send a message to the list) does not conflict with other SDL numbers nor with any subscriber's number.

SDLs can have members that are other lists as well as subscribers. Although you can configure an SDL without an authorized sender, messages must have at least one authorized sender.

To delete an SDL, use the **no list** *number* command in list-manager mode.

## Prerequisites

- An unique SDL number. This is the number an authorized sender dials to address a message to the SDL. It is a numeric string of 1-16 digits.
- (Optional) The SDL name is an alphanumeric string. If you use this variable, the name will be validated against the names of existing SDLs.
- The authorized sender is identified by an E.164 format number; the system will accept any authorized sender, even one whose number is not in the subscriber directory.
- SDL members can be subscribers or other lists. Each one is identified by a number. The system will accept any subscriber as a member, even one whose number it does not find in the subscriber directory. However, it will not accept lists that do not exist as members.

### SUMMARY STEPS

1. **list-manager**
2. **list** { **number** *number* | **publish** [ *location-id* ]}
3. **name** *string*
4. **privilege** *number*
5. **member** *number* **type** [ *sub* | *list* ]
6. **member** *number* **type** [ *sub* | *list* ]
7. **end**
8. **show list** [ *number* | *name* ] |
9. **list** { **number** *number* | **publish** [ *location-id* ]}
10. **end**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **list**<br><br>**Example:**<br>umg-1# list | Enters list manager mode. |
| **Step 2** | **list** { **number** *number* \| **publish** [ *location-id* ]}<br><br>**Example:**<br>umg-1(listmgr)# list number 1111 | Publishes lists to other messaging gateways or enters list manager mode and specifies an already existing list or creates a list. |
| **Step 3** | **name** *string*<br><br>**Example:**<br>umg-1(listmgr-edit)# name FirstList | Names a list. |
| **Step 4** | **privilege** *number*<br><br>**Example:**<br>umg-1(listmgr-edit)# privilege 4085550100 | Grants a list member permission to send messages to the list. |
| **Step 5** | **member** *number* **type** [ *sub* \| *list* ]<br><br>**Example:**<br>umg-1(listmgr-edit)# member 4085550101 type sub | Specifies a list member and its type. |
| **Step 6** | **member** *number* **type** [ *sub* \| *list* ]<br><br>**Example:**<br>umg-1(listmgr-edit)# member 2222 type list | Specifies a list member and its type. |
| **Step 7** | **end**<br><br>**Example:**<br>umg-1(listmgr-edit)# end | Exits list manager mode. |
| **Step 8** | **show list** [ *number* \| *name* ] \|<br><br>**Example:**<br>umg-1(listmgr)# show list | Displays all lists. |
| **Step 9** | **list** { **number** *number* \| **publish** [ *location-id* ]}<br><br>**Example:**<br>umg-1(listmgr)# list publish | Publishes lists to other messaging gateways or enters list manager mode and specifies an already existing list or creates a list. |
| **Step 10** | **end**<br><br>**Example:**<br>umg-1(listmgr)# end | Exits list manager mode. |

## Examples

The first example shows the output when the system fails to lock the SDLs. The second shows the out-of-sync warning, and illustrates list creation and publication.

```
umg-1# list
Locking system distribution lists...Lock manager reports failure [FAILED]
umg-1#


umg-1# list
Locking system distribution lists...[OK]

 **WARNING** This UMG is out of sync and contains old information, user should probably
publish to this UMG from a peer.
  SDL-Version                Last-Updated             List-Of-Remote-Gateways
  -------------------------  ------------------------ -----------------------
  * 50000_20070807033625     Aug 7, 2007 3:36:25 AM   51000
  -------------------------  ------------------------ -----------------------
umg-1(listmgr)# list number 1111
umg-1(listmgr-edit)# name FirstList
umg-1(listmgr-edit)# end
umg-1(listmgr)# list number 2222
umg-1(listmgr-edit)# SecondList
umg-1(listmgr-edit)# end
umg-1(listmgr)# list number 1111
umg-1(listmgr-edit)# privilege 4085550100
This authorized sender [4085550100] will be added.  However this authorized sender does
not exist yet!
umg-1(listmgr-edit)# member 4085550101 type sub
WARNING! The subscriber has been added to the list, but it doesn't exist in the subscriber
directory.

umg-1(listmgr-edit)# member 2222 type list
umg-1(listmgr-edit)# end
umg-1(listmgr)# show list
The version of system distribution list is 50000_20070815050633.

A total of 2 System Distribution List(s) have been found:

Extension      Name
-----------------------------------------------
1111           FirstList
2222           SecondList

umg-1(listmgr)# show list 1111
Extension:         1111
Name:              FirstList
Number of members: 2
Member(s):   4085550101 (subscriber)
             2222 (list)
             # of members: 2

umg-1(listmgr)# list publish
LocationID        Status          Description
-------------------------------------------------------------
51000             Published
59000             Locked(Renewed)


# of network gateways published:        1
# of network gateways failed to publish:1

umg-1(listmgr)# end
```

```
umg-1#
```

# Managing System Broadcasts

You can enable a subscriber to send a system broadcast message (SBM) to all subscribers on a specified endpoint, whether local or remote. If you grant to one subscriber the broadcast privilege for all endpoints, that person can reach all subscribers in the system by sending the same message. In Cisco UMG 1.0, this means a single SBM sent to each endpoint in succession, not one SBM sent simultaneously to all endpoints.

When you configure a broadcast VPIM ID on Cisco Unity Express 3.1 and later versions, Cisco UMG automatically picks it up when the endpoint autoregisters.

For endpoints running Cisco Unity Express 3.0 or earlier versions, not only must you configure the broadcast VPIM ID on the endpoint itself, you must also configure it on Cisco UMG when you manually provision the endpoint.

**Note** Avaya Interchange does not support SBMs.

You must create at least one authorized sender (i.e., grant a broadcast privilege) for each endpoint, otherwise no subscriber can send any messages to it.

Assign broadcast location privileges to local endpoints only because Cisco UMG only validates them locally. In other words, the configuring messaging gateway should be the endpoint's primary or secondary messaging gateway.

## Prerequisites

- The broadcast VPIM ID for each Cisco Unity Express endpoint (read it off the configured endpoint).
- The telephone number of at least one subscriber who is to be granted the system broadcast privilege for that endpoint. The authorized sender can be associated with any endpoint in the Cisco UMG network.

### SUMMARY STEPS

1. **config t**
2. **endpoint** *location-id* {**unity** | **interchange** | **cue** }
3. **broadcast-id** *broadcast-id*
4. **end**
5. **broadcast location** *location-id* **privilege**
6. **end**
7. **show endpoint local** *location-id*
8. **show broadcast location** *location-id* **privilege**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **config t**<br><br>**Example:**<br>umg-1# config t | Enters configuration mode. |
| **Step 2** | **endpoint** *location-id* **{unity \| interchange \| cue }**<br><br>**Example:**<br>umg-1(config)# endpoint 11 cue | Enters endpoint configuration mode and specifies the endpoint to be provisioned, including its type. |
| **Step 3** | **broadcast-id** *broadcast-id*<br><br>**Example:**<br>umg-1(config-endpoint)# broadcast-id 0100 | Configures the VPIM broadcast ID of the endpoint. |
| **Step 4** | **end**<br><br>**Example:**<br>umg-1(config-endpoint)# end | Exits endpoint configuration mode. |
| **Step 5** | **broadcast location** *location-id* **privilege** *number*<br><br>**Example:**<br>umg-1(config)# broadcast location 11 privilege 4085550101 | Creates an authorized sender for SBMs to the specified endpoint. |
| **Step 6** | **end**<br><br>**Example:**<br>umg-1(config)# end | Exits configuration mode. |
| **Step 7** | **show endpoint {local [** *location-id* **] \| network [** *location-id* **]}**<br><br>**Example:**<br>umg-1# show endpoint local 11 | Displays details of the specified endpoint, including and in particular, its broadcast-id. |
| **Step 8** | **show broadcast location** *location-id* **privilege**<br><br>**Example:**<br>umg-1# show broadcast location 11 privilege | Displays the authorized sender for this endpoint. |

## Examples

```
umg-1# config t
umg-1(config)# endpoint 11 cue
umg-1(config-endpoint)# broadcast-id 0100
umg-1(config-endpoint)# end
umg-1(config)# broadcast location 11 privilege 4085550101
umg-1(config)# end
umg-1# show endpoint local 11
Location Id:           11
Hostname:              Wally
Domain:                cuesim1
Prefix:                408555
NAT:                   Disabled
Type:                  CUE
Broadcast VPIM ID:     0100
Primary Gateway ID:    50000
Secondary Gateway ID:
Status:                Auto-Registered-Offline

umg-1# show broadcast location 11 privilege
A total of 1 Authorized Sender(s) have been found for location 11:

4085550101

umg-1#
```

# Deleting Peer Messaging Gateways

To delete a messaging-gateway, use the **no** form of the messaging-gateway command in Cisco UMG configuration mode.

In the following procedure the viewing activities are optional.

### SUMMARY STEPS

1. (Optional) **show messaging gateway**
2. (Optional) **show messaging gateway** [ *location-id* ]
3. **config t**
4. **no network messaging-gateway** *location-id*
5. **end**
6. **show messaging gateway [** *location-id* **]**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **show messaging gateway**<br><br>**Example:**<br>`umg-1# show messaging-gateway` | (Optional) Displays the location ID and hostname of any peer messaging gateways that have been configured, whether NAT is enabled for any of them, and the location ID of the current configuring messaging gateway. |
| **Step 2** | **show messaging gateway [** *location-id* **]**<br><br>**Example:**<br>`umg-1# show messaging-gateway 5` | (Optional) Displays the location ID and hostname of the specified messaging gateway. |
| **Step 3** | **config t**<br><br>**Example:**<br>`umg-1# config t` | Enters configuration mode. |
| **Step 4** | **no network messaging-gateway** *location-id*<br><br>**Example:**<br>`umg-1(config)# no network messaging-gateway 5` | Clears (deletes) specified messaging gateway. |
| **Step 5** | **end**<br><br>**Example:**<br>`umg-1(config)# end` | Enters EXEC mode. |
| **Step 6** | **show messaging gateway**<br><br>**Example:**<br>`umg-1# show messaging-gateway` | Displays the location ID and hostname of any peer messaging gateways that have been configured, whether NAT is enabled for any of them, and the location ID of the current configuring messaging gateway. |

## Examples

```
umg-1# show messaging-gateway
LocationID     Hostname                                NAT
-------------------------------------------------------------
5              www.mycompany.com                       disabled
51000          192.0.0.10                              disabled
59000          192.0.0.11                              disabled

Local Gateway ID: 50000

umg-1# show messaging-gateway 5
LocationID:    5
Hostname:      www.mycompany.com
NAT:           disabled

umg-1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
umg-1(config)# no network messaging-gateway 5
umg-1(config)# end
umg-1# show messaging-gateway
```

```
LocationID     Hostname                                NAT
-------------------------------------------------------------
51000          192.0.0.10 disabled
59000          192.0.0.11 disabled

Local Gateway ID: 50000

umg-1#
```

# Deleting or Clearing Endpoints

To delete a manually provisioned endpoint, use **no** form of the **endpoint** *location-id* { **cue** | **unity** | **interchange** } command in Cisco UMG configuration mode on the endpoint's primary messaging gateway.

To delete an autoregistered endpoint, use the following procedure on the endpoint's primary messaging gateway.

Although the endpoint will remain online, any messages it attempts to forward will be rejected by the current configuring Cisco UMG. However, the endpoint will be able to reregister after its registration period has expired unless you either block the endpoint or set up autoregistration for it on a different messaging-gateway. In this case, remember also to change the primary messaging gateway configuration on the endpoint itself.

The **clear endpoint** command triggers directory exchange with peer messaging gateways.

**Note** Cisco UMG does not display more than 250 endpoints without prompting. Use a filter to give you a better overview if you have more than a few endpoints.

## SUMMARY STEPS

1. **show endpoint local** [ *location-id* | **filter** *filter* ]
2. **clear endpoint** *location-id*
3. **show endpoint local** [ *location-id* | **filter** *filter* ]

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **show endpoint local** [ *location-id* \| **filter** *filter* ]<br><br>**Example:**<br>`umg-1# show endpoint local` | Displays all remote endpoints or details for the specified remote endpoint. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **clear endpoint** *location-id*<br><br>**Example:**<br>umg-1# clear endpoint 35 | Clears the data on the current configuring gateway for the specified endpoint. |
| **Step 3** | **show endpoint local** [ *location-id* \| **filter** *filter* ]<br><br>**Example:**<br>umg-1(config)# show endpoint local 35 | Displays all remote endpoints or details for the specified remote endpoint. |

## Examples

```
umg-1# show endpoint local
A total of 5 local endpoint(s) have been found:

Location    Location          Endpoint     Primary     Secondary
ID          Prefix            Type         Gateway     Gateway
-------------------------------------------------------------------
33          408108            CUE          50000       59000
34          408109            CUE          50000
35          408110            CUE          50000
36          408111            CUE          50000
37          408112            CUE          50000
umg-1# clear endpoint 35
Clear all data associated with endpoint 35 [confirm]
 [OK]
umg-1# show endpoint local
A total of 4 local endpoint(s) have been found:

Location    Location          Endpoint     Primary     Secondary
ID          Prefix            Type         Gateway     Gateway
-------------------------------------------------------------------
33          408108            CUE          50000       59000
34          408109            CUE          50000
36          408111            CUE          50000
37          408112            CUE          50000
umg-1# show endpoint local 35
Local endpoint with location id 35 has not been found.
```

# Blocking Endpoint Registration

Endpoints capable of autoregistering with Cisco UMG (only Cisco Unity Express 3.1 and later versions) can be prevented from registering.

The system logic implicitly allows autoregistration for all endpoints, therefore preventing autoregistration must be explicit.

## Prerequisites

The following information is required to prevent autoregistration-capable endpoints from registering.

- Location IDs for endpoints that you want to prevent from autoregistering.

## SUMMARY STEPS

1. **config t**
2. **registration**
3. **block location-id** *location-id*
4. **end**
5. **end**
6. **show registration block**

## DETAILED STEPS

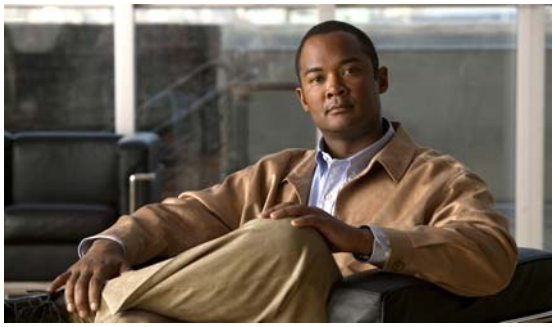
| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **config t**<br><br>**Example:**<br>`umg-1# config t` | Enters configuration mode.. |
| **Step 2** | **registration**<br><br>**Example:**<br>`umg-1(config)# registration` | Enters registration configuration mode. |
| **Step 3** | **block location-id** *location-id*<br><br>**Example:**<br>`umg-1(config-reg)# block location-id 29` | Prevents the specified endpoint from autoregistering. |
| **Step 4** | **end**<br><br>**Example:**<br>`umg-1(config-reg)# end` | Exits registration configuration mode. |
| **Step 5** | **end**<br><br>**Example:**<br>`umg-1(config)# end` | Exits configuration mode. |
| **Step 6** | **show registration block**<br><br>**Example:**<br>`umg-1# show registration block` | Displays all remote endpoints or details for the specified remote endpoint. |

**Example:**

```
umg-1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
umg-1(config)# registration
umg-1(config-reg)# block location-id 34
umg-1(config-reg)# end
umg-1(config)# end
umg-1# show registration block
UMG registration block list :
location-id 34
umg-1#
```

# Checking Endpoint Mailboxes

To find out which mailboxes are associated with which endpoints, see "Locating and Viewing Individual Mailbox Details" on page 54.



# Troubleshooting

**Last updated: April 13, 2010**

This chapter provides guidelines and information on troubleshooting, listing common problems and solutions for them. It contains the following sections:



Also check the *Cisco Unified Messaging Gateway 1.0 Release Notes* for late-breaking information.

**Tip** Bookmark the Cisco UMG documentation page for easy access to all the documents.

# General Troubleshooting Guidelines

Cisco technical support personnel may request that you run one or more of these commands when troubleshooting a problem. Cisco technical support personnel provides additional information about the commands at that time.

**Caution** Some of these commands may impact performance of your system. We strongly recommend that you do not use these commands unless directed to do so by Cisco Technical Support.

# Hardware and Software

## Rebooting the System

When you reboot Cisco UMG, it is not necessary to reboot the router.

**Caution** However, before you reboot the router, you must perform a graceful shutdown of Cisco UMG. If you do not do this, you risk data loss and file corruption.

To perform a graceful shutdown, see *Installing Cisco Network Modules in Cisco Access Routers*.

After you reboot the router, you must also reboot Cisco UMG as well, because no calls will be routed until IP connectivity is reestablished between the Cisco UMG module and the router.

## Communicating Between Components

**Problem:** You cannot open a session with Cisco UMG.

**Explanation** Someone else is logged into the messaging gateway and concurrent logins are not permitted.

**Recommended Action** Use the **service-module integrated Service-Engine** *slot*/*port* **session clear** command to clear the TTY line.

**Problem:** You cannot change or remove the IP address or IP default-gateway configurations using the Cisco UMG CLI.

**Explanation** The IP address and IP default-gateway configurations are controlled from the Cisco IOS software.

**Recommended Action** Make the required changes from the integrated service-engine interface.

**Problem:** Service-module commands do not seem to take effect.

**Explanation** The service-module status might not be steady state. RBCP configuration messages go through only when the service-module is in steady state.

**Recommended Action** Use the **service-module integrated Service-Engine** *slot*/*port* **reload** command to reload Cisco UMG.

**Problem:** You cannot ping the internal address when using the IP unnumbered scheme.

**Explanation** The IP route table is not correct.

**Recommended Action** When using IP unnumbered, add a static route that points to the integrated service-engine interface.

**Problem:** You cannot set the speed of the terminal line from the router side or the Cisco UMG side.

**Explanation** Cisco UMG does not have a CLI command to set the speed. The speed is set to 9600, 8-N-1 on both the Cisco Unified CallManager and Cisco Unity Express sides. Although Cisco IOS software allows you to change the speed settings, the changes do not take effect.

## Online Insertion and Removal

Online insertion and removal (OIR) is possible. To remove the Cisco UMG module, you must first go offline and do a graceful shutdown. See "Going Offline, Reloading, Rebooting, Shutting Down, and Going Back Online" on page 63 and for instructions on gracefully shutting down and removing the module from its slot, see *Installing Cisco Network Modules in Cisco Access Routers*.

**Caution** To avoid data loss or file corruption, always perform a graceful shutdown of the module before power-cycling the router.

# Log and Trace Files

Logging and tracing to the hard disk is turned off by default. Executing the **log trace** command starts the log and trace functions immediately.

To check the log and trace files on the hard disk, use the **show logs** command in Cisco UMG EXEC mode. It displays the list of logs available, their size and their dates of most recent modification.

Each file has a fixed length of 10 MB, and tracing or logging stops automatically when the file reaches this length. New files overwrite the old files.

## Examples

Following is sample output:

```
umg-1# show logs
SIZE             LAST_MODIFIED_TIME                          NAME
  1225782   Mon Aug 20 16:55:39 PDT 2007          linux_session.log
     4585   Wed Aug 08 14:52:25 PDT 2007                install.log
     7883   Mon Aug 20 17:10:00 PDT 2007                      dmesg
  5000139   Mon Aug 20 13:40:37 PDT 2007          messages.log.prev
     9724   Mon Aug 20 17:10:05 PDT 2007                 syslog.log
    10418   Tue Aug 07 13:39:18 PDT 2007             sshd.log.prev
      968   Wed May 09 20:51:34 PDT 2007           dirsnapshot.log
   131357   Thu Aug 09 01:28:31 PDT 2007             shutdown.log
 51325740   Tue Aug 21 17:56:10 PDT 2007               atrace.log
     1534   Mon Aug 20 17:10:04 PDT 2007          debug_server.log
    10274   Tue Jul 31 13:32:51 PDT 2007          postgres.log.prev
     2398   Mon Aug 20 17:10:04 PDT 2007                    sshd.log
104857899   Mon Aug 20 15:13:44 PDT 2007           atrace.log.prev
     4119   Mon Aug 20 17:10:22 PDT 2007              postgres.log
     4264   Mon Aug 20 17:10:07 PDT 2007                  klog.log
   984742   Tue Aug 21 18:04:36 PDT 2007              messages.log
    55435   Wed Aug 08 14:52:06 PDT 2007       shutdown_installer.log
umg-1#
```

# Logging Commands in Cisco UMG Configuration Mode

### log console

- **log console errors** - Displays error messages (severity=3)
- **log console info** - Displays information messages (severity=6)
- **log console notice** - Displays notices (severity=5)
- **log console warning** - Displays warning messages (severity=4)

### log server

- **log server address** *a.b.c.d*

### log trace

- **log trace local enable**
- **log trace server enable**
- **log trace server url** *ftp-url*

# Logging Commands in Cisco UMG EXEC Mode

### log console monitor

- **log console monitor backuprestore backuprestore** { **conf | history | init | operation | server** }
- **log console monitor backup restore all**

### log console monitor umg

- **log console monitor umg all**
- **log console monitor umg global** { **0_crash | 1_error | 2_warn | 3_debug | 4_info | all** }
- **log console monitor umg registration** {**0_crash | 1_error | 2_warn | 3_debug | 4_info | all**}
- **log console monitor umg all**
- **log console monitor umg db** { **all | connection | query** }
- **log console monitor umg direx** { **all | message | mgmt | processor | receiver | scheduler | sender** }
- **log console monitor umg lookup** { **all | request** }
- **log console monitor umg routing** { **all | gateway | monitor | route | sender | spool** }
- **log console monitor umg sdl** { **all | cli | messaging | servlet** }
- **log console monitor umg smtp** { **all | debug | error | wire** }
- **log console monitor umg system** { **all | cli** }
- **log console monitor umg translation** { **cache | rule | all** }

### log trace

- **log trace boot**
- **log trace buffer save**

# Message Transmission

When you add new endpoints to your network, if you have trouble with the endpoints' message receiving and/or transmission capabilities, contact Cisco Support to determine whether you must use the **translation-rule** command, and if so, which form of this command you should use.

**Caution** Do not use this command unless Cisco Support explicit instructs you to do so.

Each type of endpoint that Cisco UMG supports has different validation rules for accepting messages. So that the receiving messaging systems can properly accept and play back messages, when Cisco UMG forwards messages, it manipulates the message headers or the SMTP headers to correspond to the endpoints' respective validation requirements. To perform these manipulations, Cisco UMG implements translation rules.

For each endpoint type and for Cisco UMG itself, the system applies four parameters for handling SMTP headers and four for handling message headers.

The form of the CLI sets down the following sequence of information for building the rules:

1. Message header or SMTP header
2. Endpoint type
3. from-host (src-host)
4. from-user (src-user)
5. to-host (dest-host)
6. to-user (dest-user)

The command is

**translation-rule { message | smtp }{ cue | unity | interchange | umg } { from-host** { *text* | *umg-host* } **| from-user** *umg-user* **| to-host** { *text* | *umg-host* } **| to-user** *umg-user* **}**

Therefore for each endpoint type and Cisco UMG, you have the option of configuring the same parameters for both types of headers as required.

The variables and variable definitions for SMTP headers and message headers shown in Table 12 apply to all types of endpoints and to Cisco UMG.

***Table 12 Translation Rules for SMTP Headers and Message Headers***

| Keywords with Associated Variables | Variable and Variable Definition |
|---|---|
| **from-host** { *text* \| *umg-host* } | *text*: Set source email domain value.<br>*umg-host*: Variable name used for src-host translation. |
| **from-user** *umg-user* | *umg-user:* Variable name used for src-user translation. |
| **to-host** { *text* \| *umg-host* } | *text*: Set destination email domain value.<br>*umg-host*: Variable name used for dest-host translation. |
| **to-user** *umg-user* | *umg-user*: Variable name used for dest-user translation |

After using the commands according to Cisco Support's instructions, for the new configuration to take effect, save the change to the startup configuration and reload the module.

### SUMMARY STEPS

1. **config t**
2. **translation-rule { message | smtp }{ cue | unity | interchange | umg } { from-host** { *text* | *umg-host* } **| from-user** *umg-user* **| to-host** { *text* | *umg-host* } **| to-user** *umg-use*r **}**
3. **end**
4. **show translation-rule { smtp | message }**
5. write memory

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **config t**<br><br>**Example:**<br>`umg-1# config t` | Enters configuration mode. |
| **Step 2** | **translation-rule { message \| smtp } { cue \| unity \| interchange \| umg } { from-user \| to-user \| from-host \| to-host } { umg-user \| umg-host }**<br><br>**Example:**<br>`umg-1(config)# translation-rule smtp cue from-host umg-host` | Specifies the translation rule to be used to manipulate headers for messages. |
| **Step 3** | **end**<br><br>**Example:**<br>`umg-1(config)# end` | Exits configuration mode. |
| **Step 4** | **show translation-rule { smtp \| message }**<br><br>**Example:**<br>`umg-1# show translation-rule smtp` | Displays the translation rules. |
| **Step 5** | **write memory**<br><br>**Example:**<br>`umg-1# write memory` | Saves the configuration to the startup configuration. |

## Examples

The following example illustrates the message translation rule being set for a Cisco Unity Express endpoint and saved to the startup-config. The email domain of the source of the message is to be inserted into the From field of the SMTP header.

```
umg-1# config t
umg-1(config)# translation-rule smtp cue from-host mycompany.com
```

```
Save the change to startup configuration and reload the module for the new configuration
to take effect.
umg-1(config)# end
umg-1# show translation-rule smtp
SMTP Translation Rules -
CUE
From User:                from-user
From Host:                mycompany.com
To User:                  to-user
To Host:                  to-host
UNITY
From User:                from-user
From Host:                umg-host
To User:                  to-user
To Host:                  to-host
INTERCHANGE
From User:                from-user
From Host:                umg-host
To User:                  to-user
To Host:                  to-host
UMG
From User:                from-user
From Host:                from-host
To User:                  to-user
To Host:                  to-host

umg-1# write memory
```

# Saving Configuration Changes

**Problem**: You lost some configuration data.

**Recommended Action** Copy your changes to the running configuration at frequent intervals. See "Copying Configurations" on page 59.

**Problem**: You lost configuration data when you rebooted the system.

**Explanation** You did not save the data before the reboot.

**Recommended Action** Issue a **copy running-config startup-config** command to copy your changes from the running configuration to the startup configuration. When Cisco UMG reboots, it reloads the startup configuration.

**Note** Messages are considered application data and are saved directly to the disk in the startup configuration. (They should be backed up on another server in case of a power outage or a new installation.) All other configuration changes require an explicit "save configuration" operation to preserve them in the startup configuration.

# Saving and Viewing Log Files

**Problem**: You must be able to save log files to a remote location.

**Recommended Action** Log files are saved to disk by default. You can configure Cisco UMG to store the log files on a separate server by using the **log server address** command. Also, you can copy log files on the disk to a separate server if they need to be kept for history purposes, for example:

**copy log** *filename*.**log url ftp://***ftp-user-id*:*ftp-user-passwd*@*ftp-ip-address*/*directory*

```
umg# copy log messages.log url ftp://admin:messaging@172.168.0.5/log_history
```

**Problem**: You cannot display the contents of log files.

**Recommended Action** Copy the log files from Cisco UMG to an external server and use a text editor, such as **vi**, to display the content.

# Show Commands

Use all these commands in Cisco UMG EXEC mode.

- **show crash buffer** - Prints recent kernel crash log.
- **show errors** - Displays any errors reported in the messages log.
- **show interfaces gigabitethernet *0-1*** where **gigabitethernet** conforms to IEEE 802.3 and *1-0* is the Ethernet unit number.
- **show interfaces ide *0*** where **ide** is the Integrated Drive Electronics (hard disk) and *0* is the disk unit number.
- **show log name** *word* where *word* is the name identifying the log.
- **show logging** - Displays the console logging options as follows:

***Table 13 Console Logging Options***

| **Keyword** | **Argument** | | |
|---|---|---|---|
| info: | off/on | | |
| notice: | off/on | | |
| warning: | off/on | | |
| errors: | off/on | | |
| fatal: | off/on | | |
| Monitored event Info | | | |
| Module | Entity | Activity | Filter |
| Monitored events active/No monitored events active | | | |
| Server Info: | | | |
| Log server address: | | | |

- **show logs**: Displays a list of log files.
- **show memory**: Displays memory statistics.

- **show processes cpu:** Displays CPU processes.
- **show processes memory:** Displays RAM utilization.
- **show software directory { downgrade | download }**: Displays configured software information.
- **show software download server:** Displays configured software information.
- **show software licenses**: Displays configured software information.
- **show software packages**: Displays configured software information.
- **show software versions [detail]:** Displays additional subsystem version information
- **show tech-support:** Displays complete system information.
- **show trace buffer:** Prints recent system event messages. Do not use except by permission from Cisco Technical Support.
- **show trace store:** Prints system event messages from hard-drive store - Do not use except by permission from Cisco Technical Support.
- **show store-prev** - Prints system event messages from previous hard-drive store - Do not use except by permission from Cisco Technical Support.
- **show version** - Displays the version of all hardware components.

# System Reports

Cisco UMG provides the following system reports:

- Backup and restore history: see "Backing Up Files" on page 46.
- System parameters: see "Displaying Management Data Activity" on page 56 and "Viewing System Activity Messages" on page 57.
- Memory and CPU usage: see "Log and Trace Files" on page 81

# Trace Commands

To troubleshoot network configuration in Cisco UMG, use the following commands in EXEC mode.

### trace backuprestore

- **trace backuprestore all**
- **trace backuprestore backuprestore { conf | history | init | operation | server | all }**

### trace umg

- **trace umg global { 0_crash | 1_error | 2_warn | 3_debug | 4_info | all }**
- **trace umg registration {0_crash | 1_error | 2_warn | 3_debug | 4_info | all}**
- **trace umg all**
- **trace umg db { all | connection | query }**
- **trace umg direx { all | message | mgmt | processor | receiver | scheduler | sender }**
- **trace umg lookup { all | request }**
- **trace umg routing { all | gateway | monitor | route | sender | spool }**

- **trace umg sdl { all | cli | messaging | servlet }**
- **trace umg smtp { all | debug | error | wire }**
- **trace umg system { all | cli }**
- **trace umg translation { cache | rule | all }**

#### trace all

- **trace all**

#### trace dbclient

- **trace dbclient all**
- **trace dbclient database { all | connection | execute }**
- **trace dbclient database { garbagecollect | largeobject | mgmt | query | results | transaction }**

#### trace dns

- **trace dns all**
- **trace dns cache { all | daemon | ethconfig | localzone | startup }**
- **trace dns enablecheck { all | debug | dns_check | dns_query }**
- **trace dns enablecheck { hostname_check | ipv4_check | results }**
- **trace dns resolver { all | receive | send }**
- **trace dns server { all | answer | ask }**

#### trace management

- **trace management agent {all | debug }**
- **trace management all**

#### trace ntp

- **trace ntp all**
- **trace ntp ntp { all | clkadj | clkselect | clkvalidity | clockstats | event }**
- **trace ntp ntp { loopfilter | loopstats | packets | peerstats }**

#### trace security

- **trace security all**
- **trace security policy { all | password | pin }**

#### trace snmp

- **trace snmp jni { net-snmp | all }**
- **trace snmp agent { all | debug }**
- **trace snmp all**

#### trace superthread

- **trace superthread all**
- **trace superthread main { all | startup }**
- **trace superthread parser**

**trace sysdb**

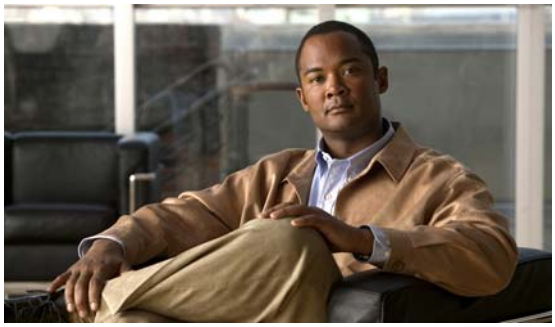
- **trace sysdb all**
- **trace sysdb consumer** { **all | get | lookup | set** }
- **trace sysdb lock** { **acquire | all | release | wait** }
- **trace sysdb producer** { **all | attrCreate | attrDelete | mkdir** }
- **trace sysdb producer** { **nodeAttach | nodeDetach | nodeHandle | rmdir** }
- **trace sysdb provider** { **all | check | get | commit | startup | stop** }
- **trace sysdb traversal** { **all | attribute | directory | node** }
- **trace sysdb utility** { **all | chdir | dealloc | metainfo | namelookup** }

**trace udppacer**

- **trace udppacer all**
- **trace udppacer udppacer** { **all | block_starve | ccncall | debug | statistics** }

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **trace dns resolver** { **all** \| **receive** \| **send** }<br><br>**Example:**<br>`umg-1# trace dns resolver all` | Enables tracing for DNS network functions.<br>• **all**—Traces every DNS activity.<br>• **receive**—Traces DNS receiving.<br>• **send**—Traces DNS sending. |
| **Step 2** | **trace sysdb all**<br><br>**Example:**<br>`umg-1# trace sysdb all` | Enables tracing for every sysdb entity and activity. |
| **Step 3** | `trace dns all`<br><br>**Example:**<br>`umg-1# trace dns all` | Enables tracing for every DNS event. For example, displays DNS lookups that are performed and results that are given when a domain is verified and resolved using SMTP. |
| **Step 4** | **trace dbclient database** { **garbagecollect** \| **largeobject** \| **mgmt** \| **query** \| **results** \| **transaction** }<br><br>**Example:**<br>`umg-1# trace dbclient database results` | Enables tracing for client database functions. The following keywords specify the type of traces:<br>• **garbagecollect**—Garbage collection process.<br>• **largeobject**—Large object reads and writes to the database.<br>• **mgmt**—Database management processes.<br>• **query**—Queries performed on the database.<br>• **results**—Results of queries, inserts, and updates.<br>• **transactions**—Start and end of database transactions. |



# Appendix A: Cisco Unity Express Endpoint Autoregistration to Cisco Unified Messaging Gateway 1.0

**Revised: April 13, 2010**

This section covers principally the new commands in Cisco Unity Express 3.1 and later versions to enable endpoints of this type to autoregister with Cisco Unified Messaging Gateway (UMG) 1.0.

Endpoints running Cisco Unity Express 3.0 or earlier versions do not support autoregistration. They must be manually configured on Cisco UMG.

An endpoint of the type Cisco Unity Express 3.1 and later versions that does not autoregister will be treated as if it were Cisco Unity Express 3.0 or earlier versions.

The section contains the following topics:



## Overview of the Autoregistration Process

The purpose of autoregistration is for Cisco UMG to automatically “discover” legitimate endpoints of the type Cisco Unity Express 3.1 and later versions. (

**Note** The only type of endpoint that can autoregister is Cisco Unity Express 3.1 and later versions. In this appendix, the term ‘endpoint’ refers exclusively to that type of endpoint, unless otherwise specified.

A messaging gateway discovers whether an endpoint is legitimate by attempting to validate the shared secret information in the autoregistration message sent by the endpoint. Successful validation ensures that messages can only be exchanged between trusted peers.

The autoregistration process starts after the endpoint boots up. An appropriately configured endpoint is enabled to autoregister and it has the following information:

- The location ID and IP address or domain name of its primary (and where applicable, its secondary) messaging gateway
- Registration ID and password that the messaging gateways will be expecting
  - The instructions for configuring this ID and password on Cisco UMG are given in "Configuring Endpoint Autoregistration Support" on page 28.
  - The instructions for configuring this ID and password on Cisco Unity Express 3.1 and later versions are given below, in "Configuring Cisco Unity Express 3.1 and later versions Autoregistration with Cisco UMG" on page 92.

Beginning the process, the endpoint sends registration requests to both the primary Cisco UMG and the secondary messaging gateway in that order, if a secondary is configured.

**Note** If autoregistration for the primary messaging gateway fails cue to incorrect configuration, the endpoint does not attempt to proceed with the secondary messaging gateway. However, if connectivity problems prevent the endpoint from contacting the primary messaging gateway, the endpoint does try to reach the secondary messaging gateway.

In the registration message is information about itself, such as its own location ID, broadcast ID, and so on. If the primary messaging gateway encounters configuration problems during registration (for example, a missing location-id), the process will fail, and the endpoint will not try to register with the secondary messaging gateway. If the problems are of a different nature (for example, connectivity problems) the endpoint will go ahead and try to register with the secondary messaging gateway.

When the endpoint autoregisters, the messaging gateway adds the endpoint to a trusted endpoints table and the endpoint is then allowed to send and receive VPIM messages to and from the messaging gateway with which it has registered, as well as to retrieve remote user information.

Automatic directory information exchange takes place a couple of minutes after registration, thereby enabling the messaging gateway to learn about the endpoint's properties.

Endpoints of the types Cisco Unity Express 3.0 or earlier versions, Cisco Unity, and Avaya Interchange do not support autoregistration, so they must be individually provisioned from messaging gateways. Instructions for doing this are given in "Provisioning Endpoints Manually" on page 31. An endpoint running Cisco Unity Express 3.1 and later versions that is not enabled to autoregister will be treated the same as these other types of endpoint.

# Configuring Cisco Unity Express 3.1 and later versions Autoregistration with Cisco UMG

An endpoint running Cisco Unity Express 3.1 and later versions or later can autoregister with Cisco Unified Messaging Gateway. This means that when the endpoint comes online (or when you use the **messaging-gateway registration** command), it seeks out its messaging gateway(s), if configured) and registers itself. The alternative is manual provisioning, which entails configuring all relevant details for each endpoint on its messaging gateway. This is the only option available to supported endpoints not running Cisco Unity Express 3.1 and later versions.

After an endpoint autoregisters, its messaging gateway exchanges directories with its peers so that the whole system becomes aware that this endpoint is now online. After the endpoint administrator enables autoregistration, any time either the endpoint or the messaging gateway goes offline, the endpoint will re-register automatically as soon as both come back online.

Before enabling autoregistration, the administrator for Cisco Unity Express 3.1 and later versions must specify the primary (and optionally the secondary) messaging gateway access information. Using these commands on the endpoint causes the profile(s) for the messaging gateways to be stored in the endpoint's running-config.

**Caution** You must copy these configurations to the startup-config to make them persistent.

## SUMMARY STEPS

1. **config t**
2. **messaging-gateway primary** *location-id* { *umg-ip-addr* | *umg-hostname* }
3. **username** *user* **password** { **text** | **encrypted** } *password*
4. (Optional) **retry-interval** *integer*
5. (Optional) **nat** { **http** | **vpim** } *a.b.c.d integer*
6. **end**
7. (Optional) **messaging-gateway secondary** *location-id* { *umg-ip-addr* | *umg-hostname* }
8. (Optional) **username** *user* **password** { **text** | **encrypted** } *password*
9. (Optional) **retry-interval** *integer*
10. (Optional) **nat** { **http** | **vpim** } *a.b.c.d integer*
11. **end**
12. messaging-gateway registration
13. end
14. show messaging-gateway

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **config t**<br><br>**Example:**<br>`se-10-0-0-0# config t` | Enters configuration mode. |
| **Step 2** | **messaging-gateway primary** *location-id* **{** *umg-ip-addr* **\|** *umg-hostname* **}**<br><br>**Example:**<br>`se-10-0-0-0(config)# messaging-gateway primary 100 192.0.2.21` | Enters messaging gateway configuration mode and specifies the following information for the primary messaging gateway:<br>• *location-id*--the location-id of the primary messaging gateway<br>• *umg-ip-addr* **\|** *umg-hostname*--the IP address or hostname of the primary messaging gateway<br>Configure the primary messaging gateway before the secondary. If you do not, you will get the error message "Primary messaging gateway needs to be configured first." |
| **Step 3** | **username** *user* **password** { **text** \| **encrypted** } *password*<br><br>**Example:**<br>`se-10-0-0-0(config-messaging-gateway)# username cue31 password text herein` | Specifies the username and password required to autoregister with the messaging gateway. Note that the username is not necessarily the same as the endpoint's location ID, because the Cisco UMG administrator can configure a messaging gateway to expect the same username from multiple endpoints. |
| **Step 4** | **retry-interval** *integer*<br><br>**Example:**<br>se-10-0-0-0(config-messaging-gateway)# retry-interval 2 | (Optional) The retry-interval is the delay in minutes before the endpoint attempts to reregister with the messaging gateway. The default is 5 minutes, range 0 - 65535. |
| **Step 5** | nat { **http** *a.b.c.d integer* **\| vpim** *a.b.c.d integer* **}**<br><br>**Example:**<br>se-10-0-0-0(config-messaging-gateway)# nat http 192.0.2.22 80 | (Optional) Configures HTTP or VPIM NAT for the specified messaging gateway. Integer is the HTTP or the VPIM port, range 1 - 65535. |
| **Step 6** | **end**<br><br>**Example:**<br>`se-10-0-0-0(config-messaging-gateway)# end` | Exits messaging gateway configuration mode and enters config mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 7** | **messaging-gateway secondary** *location-id* { *umg-ip-addr* \| *umg-hostname* }<br><br>**Example:**<br>`se-10-0-0-0(config)# messaging-gateway secondary 101 192.0.2.21` | (Optional) Enters messaging gateway configuration mode and specifies the following information for the secondary messaging gateway:<br>• *location-id*--the location-id of the secondary messaging gateway<br>• *umg-ip-addr* \| *umg-hostname*--the IP address or hostname of the secondary messaging gateway<br>Configure the primary messaging gateway before the secondary. If you do not, you will get the error message "Primary messaging gateway needs to be configured first." |
| **Step 8** | **username** *user* **password** { **text** \| **encrypted** } *password*<br><br>**Example:**<br>`se-10-0-0-0(config-messaging-gateway)# username cue32 password text herein` | Specifies the username and password required to autoregister with the messaging gateway. Note that the username is not necessarily the same as the endpoint's location ID, because the Cisco UMG administrator can configure a messaging gateway to expect the same username from multiple endpoints. |
| **Step 9** | **retry-interval** *integer*<br><br>**Example:**<br>se-10-0-0-0(config-messaging-gateway)# retry-interval 2 | (Optional) The retry-interval is the delay in minutes before the endpoint attempts to reregister with the messaging gateway. The default is 5 minutes, range 0 - 65535. |
| **Step 10** | nat { **http** *a.b.c.d integer* \| **vpim** *a.b.c.d integer* }<br><br>**Example:**<br>se-10-0-0-0(config-messaging-gateway)# nat vpim 192.0.2.23 9925 | (Optional) Configures HTTP or VPIM NAT for the specified messaging gateway. Integer is the HTTP or the VPIM port, range 1 - 65535. |
| **Step 11** | **end**<br><br>**Example:**<br>`se-10-0-0-0(config-messaging-gateway)# end` | Exits messaging gateway configuration mode. |
| **Step 12** | messaging-gateway registration<br><br>**Example:**<br>se-10-0-0-0(config)# messaging-gateway registration | Causes the endpoint to send a registration message to its primary and, if applicable, to its secondary messaging gateway, unless registration with the primary fails due to a configuration error. |
| **Step 13** | end<br><br>**Example:**<br>se-10-0-0-0(config)# end | Exits config mode and enters EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 14** | show messaging-gateway<br><br>**Example:**<br>se-10-0-0-0# show messaging-gateway | (Optional) Displays the details associated with the registration with the messaging gateway, successful or otherwise. For more information, see the "Verifying the Registration Status of a Cisco Unity Express 3.1 Endpoint" section on page 102. |
| **Step 15** | write memory<br><br>**Example:**<br>se-10-0-0-0# write memory | Copies the running-config to the startup-config. |

## Example

The following commands on a Cisco Unity Express 3.1 and later versions endpoint set it up to autoregister with Cisco UMG, and then enable autoregistration and finally write the configuration to startup-config.

```
se-10-0-0-0# config t
se-10-0-0-0(config)# messaging-gateway primary 100 192.0.2.0
se-10-0-0-0(config-messaging-gateway)# username cue31 password text herein
se-10-0-0-0(config-messaging-gateway)# retry-interval 2
se-10-0-0-0(config-messaging-gateway)# nat http 192.0.2.22 80
se-10-0-0-0(config-messaging-gateway)# end
se-10-0-0-0(config)# messaging-gateway secondary 101 192.0.2.21
se-10-0-0-0(config-messaging-gateway)# username cue32 password text herein
se-10-0-0-0(config-messaging-gateway)# retry-interval 2
se-10-0-0-0(cconfig-messaging-gateway)# nat vpim 192.0.2.23 9925
se-10-0-0-0(config-messaging-gateway)# end
se-10-0-0-0(config)# messaging-gateway registration
se-10-0-0-0(config)# end
se-10-0-0-0> show messaging-gateway
Messaging gateways :
AutoRegister to gateway(s) : Enabled
Remote directory lookup : Enabled (without TUI prompt)
Primary messaging gateway :
        192.0.2.0
        nat http 192.0.2.22 (80)
        Status : Registered (Wed Sep 19 18:04:45 PDT 2007)
        Reg-expiration : Thu Sep 20 18:04:45 PDT 2007
        Default route : Disabled
        Location-id : 100
        Reg-id : cue31
        Reg-password : (Not displayed)
        Retry-interval : 2 minute(s)
Secondary messaging gateway :
        192.0.2.21
        nat http 10.1.3.150 (80)
        nat vpim 192.0.2.23 (9925)
        Status : Registered (Wed Sep 19 18:04:45 PDT 2007)
        Reg-expiration : Thu Sep 20 18:04:45 PDT 2007
        Default route : Disabled
        Location-id : 101
        Reg-id : cue32
        Reg-password : (Not displayed)
        Retry-interval : 2 minute(s)
se-10-0-0-0> write memory
```

# Manually Registering a Cisco Unity Express Endpoint

If you want to add a Cisco Unity Express endpoint to your Cisco UMG system, and

- it is running Cisco Unity Express 3.0 or earlier versions, or
- you want to avoid autoregistration activity with an endpoint running Cisco Unity Express 3.1 and later versions,

you must manually provision it from Cisco UMG.

Configure the endpoint following the instructions in the Cisco Unity Express documentation. Reproduced below is the relevant section of it, “Configuring Network Locations” from the Cisco Unity Express 2.3 CLI Administrator Guide. This is for orientation only.

**Note** You must perform the steps only if the endpoint has never undergone initial configuration - if the endpoint is already in operation, you will already have done all this.

## SUMMARY STEPS

1. **config t**
2. **network location-id** *number*
3. (Optional) **name** *location-name*
4. (Optional) **abbreviation** *name*
5. **email domain** *domain-name*
6. **voicemail phone-prefix** *digit string*
7. (Optional) **voicemail extension-length** *number* [**min** *number* | **max** *number*]
8. (Optional) **voicemail vpim-encoding** {**dynamic | G711ulaw | G726**}
9. (Optional) voicemail spoken-name
10. end

Repeat Steps 2 through 10 for each remote location.

11. **network local location-id** *number*
12. end
13. **show network locations configured**
14. **show network detail location-id** *number*
15. **show network detail local**
16. **show network queues**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | `config t`<br><br>**Example:**<br>`se-10-0-0-0# config t` | Enters configuration mode. |
| **Step 2** | `network location-id` *number*<br><br>**Example:**<br>`se-10-0-0-0(config)# network location-id 9` | Enters location configuration mode to allow you to add or modify a location.<br>• *number*—A unique numeric ID assigned to the location. This number is used to identify the location and is entered when a subscriber performs addressing functions in the TUI. The maximum length of the number is 7 digits. Cisco Unity Express supports up to 500 locations on a single system.<br>• To delete a location, use the **no** form of this command. |
| **Step 3** | **name** *location-name*<br><br>**Example:**<br>`se-10-0-0-0(config-location)# name "San Jose"` | (Optional) Descriptive name used to identify the location. Enclose the name in double quotes if spaces are used.<br>• To delete a location name description, use the **no** form of this command. |
| **Step 4** | **abbreviation** *name*<br><br>**Example:**<br>`se-10-0-0-0(config-location)# abbreviation sjcal` | (Optional) Creates an alphanumeric abbreviation for the location that is spoken to a subscriber when the subscriber performs addressing functions in the TUI. You cannot enter more than 5 characters.<br>• To delete an abbreviation, use the **no** form of this command. |
| **Step 5** | **email domain** *domain-name*<br><br>**Example:**<br>`se-10-0-0-0(config-location)# email domain mycompany.com` | Configures the e-mail domain name or IP address for the location. The domain name is added when sending a VPIM message to the remote location (for example, "4843000@mycompany.com"). If you do not configure a domain name or IP address, the Cisco Unity Express system at this location cannot receive network messages.<br>• To remove the e-mail domain name or IP address and disable networking, use the **no** form of this command.<br><br>**Caution** If you remove the e-mail domain for a network location, the system automatically disables networking from the Cisco Unity Express module to that location.<br>If you remove the e-mail domain for the local location, then networking on that Cisco Unity Express module is disabled.<br>To reenable a location, assign it a valid e-mail domain. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **voicemail phone-prefix** *digit-string*<br><br>**Example:**<br>`se-10-0-0-0(config-location)# voicemail phone-prefix 484` | (Optional) Configures the phone number prefix that is added to an extension to create a VPIM address for a subscriber at the location. A prefix is required only if an e-mail domain services multiple locations and extensions between the locations are not unique. Valid values: 1 to 15 digits. Default value: empty.<br>• To delete a phone prefix, use the **no** form of this command. |
| **Step 7** | **voicemail extension-length** {*number* \| **min** *number* **max** *number*}<br><br>**Example:**<br>`se-10-0-0-0(config-location)# voicemail extension-length 8`<br><br>`se-10-0-0-0(config-location)# voicemail extension-length min 5 max 9` | (Optional) Configures the voice mail extension length for the location.<br>• *number*—Configures the number of digits contained in extensions at the location.<br>• **max** *number*—Sets the minimum number of digits for extensions. Default value: 2.<br>• **min** *number*—Sets the maximum number of digits for extensions. Default value: 15.<br>• To remove the configuration for the number of digits for extensions, use the **no** form of this command. |
| **Step 8** | **voicemail vpim-encoding** {**dynamic** \| **G711ulaw** \| **G726**}<br><br>**Example:**<br>`se-10-0-0-0(config-location)# voicemail vpim-encoding G711ulaw` | (Optional) Configures the encoding method used to transfer voice-mail messages to this location.<br>• **dynamic**—Cisco Unity Express negotiates with the location to determine the encoding method<br>• **G711ulaw**—Cisco Unity Express always sends messages as G711 mu-law .wav files. Set this only if the receiving system supports G711 mu-law encoding (such as Cisco Unity).<br>• **G726**—Cisco Unity Express always sends messages as G726 (32K ADPCM). Use for low-bandwidth connections or when the system to which Cisco Unity Express is connecting does not support G711 u-law.<br>• Default value: **dynamic**.<br>• To return to the default value for encoding, use the **no** or **default** form of this command. |
| **Step 9** | `voicemail spoken-name`<br><br>**Example:**<br>`se-10-0-0-0(config-location)# voicemail spoken-name` | (Optional) Enables sending the spoken name of the voice-mail originator as part of the message. If the spoken name is sent, it is played as the first part of the received message. Default: enabled.<br>• To disable sending the spoken name, use the **no** form of this command. |
| **Step 10** | `end`<br><br>**Example:**<br>`se-10-0-0-0(config-location)# end` | Exits location configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 11** | **network local location-id** *number*<br><br>**Example:**<br>`se-10-0-0-0(config)# network local location-id 1` | Enables networking for the local Cisco Unity Express system identified by the location-id number.<br>• To delete the local location, use the **no** form of this command.<br><br>**Caution** If you delete the local network location and then save your configuration, when you reload Cisco Unity Express, the local network location will remain disabled. After Cisco Unity Express restarts, reenter the **network local location-id** command to reenable networking at this location. |
| **Step 12** | **exit**<br><br>**Example:**<br>`se-10-0-0-0(config)# exit` | Exits configuration mode. |
| **Step 13** | `show network locations configured`<br><br>**Example:**<br>`se-10-0-0-0# show network locations configured` | (Optional) Displays the location-id, name, abbreviation, and domain name for each configured Cisco Unity Express location. |
| **Step 14** | **show network detail location-id** *number*<br><br>**Example:**<br>`se-10-0-0-0# show network detail location-id 9` | (Optional) Displays network information for the specified location-id, including the number of messages sent and received. |
| **Step 15** | **show network detail local**<br><br>**Example:**<br>`se-10-0-0-0# show network detail local` | (Optional) Displays network information for the local Cisco Unity Express location, including the number of messages sent and received. |
| **Step 16** | **show network queues**<br><br>**Example:**<br>`se-10-0-0-0# show network queues` | (Optional) Displays information about messages in the outgoing queue that are to be sent from this Cisco Unity Express system. The queue information contains three displays: one for urgent job queue information, one for normal job queue information, and one for running job information. |

# Examples

The following examples illustrate the output from the **show network** commands on company Mycompany's call control system in San Jose with remote voice-mail provided by six remote Cisco Unity Express sites.

```
se-10-0-0-0# show network locations

ID        NAME                          ABBREV  DOMAIN
101       'San Jose'                      SJC    sjc.mycompany.com
102       'Dallas/Fort Worth'             DFW    dfw.mycompany.com
201       'Los Angeles'                   LAX    lax.mycompany.com
202       'Canada'                        CAN    can.mycompany.com
```

```
301       'Chicago'                       CHI    chi.mycompany.com
302       'New York'                      NYC    nyc.mycompany.com
401       'Bangalore'                     BAN    bang.mycompany.com

se-10-0-0-0# show network detail location-id 102

Name:                                Dallas/Fort Worth
Abbreviation:                        DFW
Email domain:                        dfw.mycompany.com
Minimum extension length:            2
Maximum extension length:            15
Phone prefix:
VPIM encoding:                        G726
Send spoken name:                     enabled
Sent msg count:                       10
Received msg count:                   110

se-10-0-0-0# show network detail local

location-id:                          101
Name:                                 San Jose
Abbreviation:                         SJC
Email domain:                         sjc.mycompany.com
Minimum extension length:             2
Maximum extension length:             15
Phone prefix:
VPIM encoding:                        dynamic
Send spoken name:                     enabled
```

The following example illustrates output from the **show network queues** command. The output includes the following fields:

- ID—Job ID.
- Retry—Number of times that Cisco Unity Express has tried to send this job to the remote location.
- Time—Time when the job will be resent.

```
se-10-0-0-0# show network queues

Running Job Queue
=================

ID    TYPE TIME       RETRY SENDER          RECIPIENT
107   VPIM 06:13:26   20    jennifer        1001@sjc.mycompany.com
106   VPIM 06:28:25   20    jennifer        1001@sjc.mycompany.com

Urgent Job Queue
=================

ID    TYPE TIME       RETRY SENDER          RECIPIENT
123   VPIM 16:33:39   1     andy            9003@lax.mycompany.com

Normal Job Queue
=================

ID    TYPE TIME       RETRY SENDER          RECIPIENT
122   VPIM 16:33:23   1     andy            9001@lax.mycompany.com
124   VPIM 16:34:28   1     andy            9003@lax.mycompany.com
125   VPIM 16:34:57   1     andy            9002@lax.mycompany.com
126   VPIM 16:35:43   1     andy            9004@lax.mycompany.com
```

# Verifying the Registration Status of a Cisco Unity Express 3.1 Endpoint

You can verify whether the current Cisco Unity Express 3.1 and later versions endpoint is registered with a messaging gateway, and check all the details associated with the registration - successful or otherwise - by using the **show messaging-gateway** command in Cisco Unity Express EXEC mode.

You can see which Cisco UMGs you have configured as its primary and secondary messaging gateways, with their respective port numbers. Indications in the status column show whether or not the endpoint has registered with the messaging gateway successfully.

***Table 14 show messaging-gateway Output***

| | | | |
|---|---|---|---|
| AutoRegister to messaging gateway(s) | Enabled / disabled | | |
| Remote directory lookup | Enabled / disabled | with / without TUI prompt | |
| Primary/secondary messaging gateway | IP address (port number) | | |
| | Status | Registered / Not Registered | If registered, timestamp of initial registration confirmation; if not registered, reason is given as a code (see Table 15) |
| | Default route | Enabled/ disabled | |
| | Location-id | location-id of the messaging gateway | |
| | Reg-id | Registration username the Cisco UMG expects from endpoint | |
| | Reg-password | (Not displayed) | Registration password the Cisco UMG expects from endpoint. It is never displayed. |
| | **Retry-interval** | Delay in minutes before the endpoint attempts to register again. Default is 5 minutes. | Not displayed if not set. |

If the endpoint has registered successfully, you will see the date and time of the initial registration in the status column. You can also check the configuration for a default routing destination for a message to a voicemail address that can be resolved by neither Cisco Unity Express nor Cisco UMG. To illustrate: if you give a phone number that cannot be found in a Cisco Unity Express local search or in a Cisco UMG remote lookup, the message will be forwarded to that default route destination.

If the endpoint has not registered successful, the reason for the failure will be displayed in the status column.

*Table 15 show messaging-gateway: Status Codes*

| Code | Meaning |
|---|---|
| Registered | |
| Not registered | Autoregistration is not enabled |
| Not configured | |
| Not registered (general error) | Autoregistration failed due to an error other than those specified in this table. |
| Not registered (connection timeout) | Connection timed out |
| Not registered (authentication failed) | Authentication failed |
| Not registered (link is down) | Link is down |
| Not registered (location is forbidden) | The Cisco Unity Express endpoint with that location-id has been blocked by Cisco UMG and is thus is not allowed to register (for instructions on how to prevent an endpoint from registering, see "Configuring Endpoint Autoregistration Support" on page 28). |
| Not Registered (duplicated location) | The Cisco Unity Express location ID is not globally unique: there is another entity in the system with the same location-id. |
| Not Registered (invalid configuration) | General configuration error such as the secondary messaging gateway location ID not being configured on the primary messaging gateway. |
| Not Registered (manually de-registered) | An intermediate state to indicate manually triggered re-registration, for example, the messaging gateway's access information being updated. |

# Enabling or Disabling Remote Lookup, With or Without TUI Confirmation

## Enabling Remote Directory Lookup Without TUI Prompt

When you enable autoregistration by issuing the **messaging-gateway registration** command on a Cisco Unity Express 3.1 and later versions endpoint, you also enable the endpoint to do remote lookup automatically. This includes a short prompt informing subscribers that the lookup may take some time.

## Enabling Remote Directory Lookup With TUI Prompt

Enabling the remote directory lookup feature does not also enable the directory lookup confirmation in the TUI flow feature, in which Cisco Unity Express 3.1 and later versions gives subscribers the option to do remote lookup if there is no local match. To enable TUI directory lookup confirmation, use the config-mode command **messaging-gateway directory lookup tui-prompt**.

### Disabling Remote Directory Lookup

To have no remote lookup at all, disable it by issuing the **no messaging-gateway directory lookup** command.

**Note** Disabling the remote directory lookup feature also disables directory lookup confirmation in the TUI flow, and conversely, enabling directory lookup confirmation in the TUI flow will also enable remote directory lookup.

### Viewing Status

To view the status of these features, use the **show messaging-gateway** command, which displays the following output:

Remote directory lookup status:

- No--remote directory lookup is disabled
- Yes--remote directory lookup is enabled
  - Enabled with TUI-prompt--TUI confirmation prompt is enabled
  - Enabled without TUI-prompt--TUI confirmation prompt is disabled.

# Viewing Cached and/or Configured Network Locations

To view a list of all cached remote location entries on Cisco Unity Express 3.1 and later versions, use the EXEC-mode **show network locations cached** command.

To list all configured remote location entries on Cisco Unity Express 3.1 and later versions, use the EXEC-mode **show network locations configured** command. This command replaces the old **show network locations** command.

# Refreshing Locations

To manually refresh a cached location entry on Cisco Unity Express 3.1 and later versions, use the **network location cache refresh** *id* command in EXEC-mode. This command will not generate any response if it is performed successfully. Otherwise, an error message appears.

# Setting the Expiration for Cached Locations

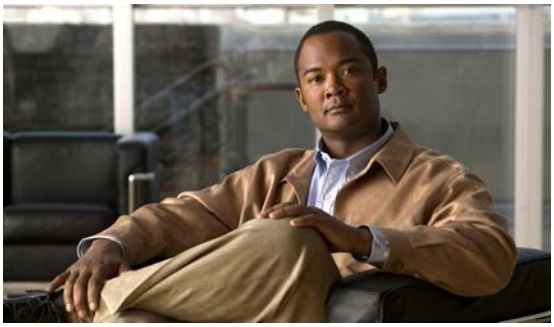
To set the expiration time for a cached location on Cisco Unity Express 3.1 and later versions, use the **network location cache expiry** *int* command in config-mode. The *int* value stands for number of days. By default, this value is set to 4. The **no** command will set the value back to its default value. The value is persisted by means of the nvgen method. It is not stored in the database.

# Overloading a NAT Device: the Consequences for Endpoints

One endpoint can be configured to get to its primary messaging gateway with complete connectivity if:

- Two Cisco Unity Express endpoints are behind a NAT device that has only one IP address to assign --an overload situation--
- Those endpoints have two different messaging gateways configured as primary messaging gateways,

**Note** The other endpoint can only do HTTP-related activities (assuming proper configuration) and not the SMTP activities.



# INDEX

## Numerics



## A



## B



## C

## D



## E



## F



## G



## I



## L



## M



## N



## O

## P



## R



## S



## T



## U